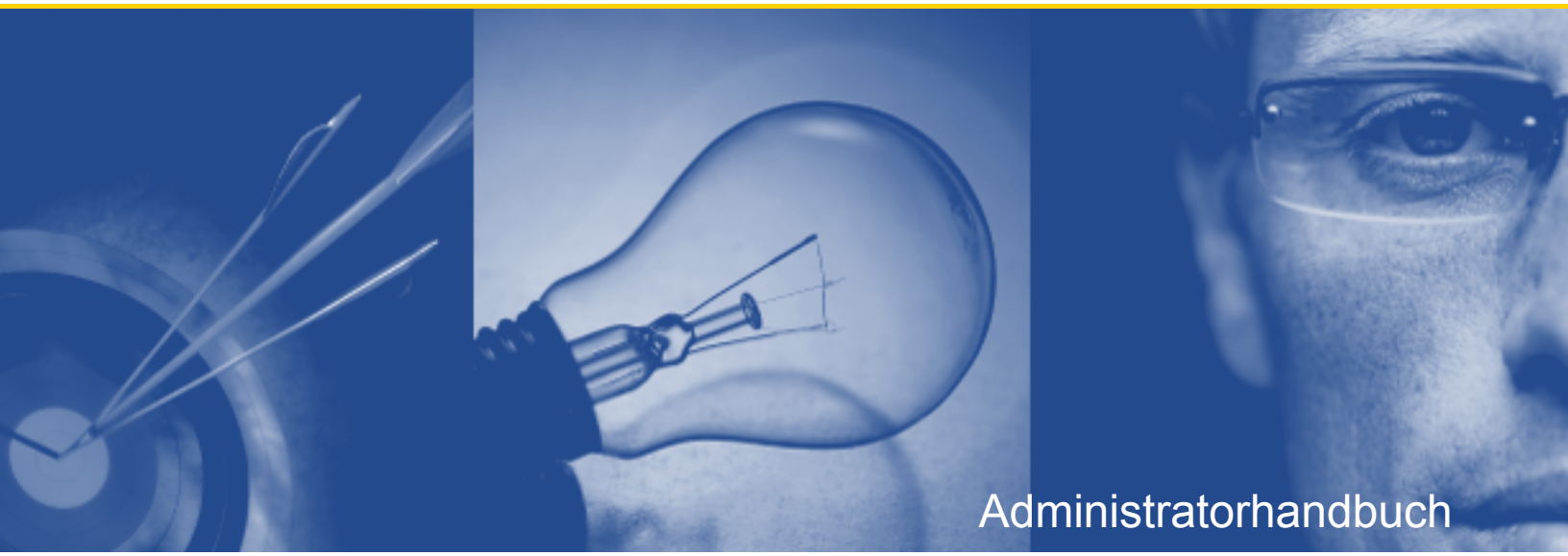
QUEST SOFTWARE®

Quest® ActiveRoles Server 6.5



Administratorhandbuch

© 2009 Quest Software, Inc.
ALLE RECHTE VORBEHALTEN.

Dieses Handbuch enthält urheberrechtlich geschützte Informationen. Die im vorliegenden Handbuch beschriebene Software unterliegt den Bedingungen der jeweiligen Softwarelizenz oder Geheimhaltungsvereinbarung. Die Software darf nur gemäß den Bestimmungen der gültigen Vereinbarung verwendet oder kopiert werden. Die Vervielfältigung und die Übermittlung des vorliegenden Handbuchs oder seiner Teile in anderen elektronischen oder gedruckten Publikationen ist ohne ausdrückliche Zustimmung von Quest Software, Inc., nicht gestattet. Dies gilt nicht, wenn die Informationen zum ausschließlichen privaten Gebrauch eines Nutzers bestimmt sind.

Bei Fragen zur möglichen Verwendung dieser Materialien wenden Sie sich bitte an:

Quest Software World Headquarters
LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656
USA
www.quest.com
E-Mail: legal@quest.com

Informationen über unsere lokalen und internationalen Büros finden Sie auf unserer Website.

Warenzeichen

Quest, Quest Software, das Quest Software-Logo, Aelita, Akonix, AppAssure, Benchmark Factory, Big Brother, ChangeAuditor, DataFactory, DeployDirector, ERDisk, Foglight, Funnel Web, GPOAdmin, I/Watch, Imceda, InLook, IntelliProfile, InTrust, Invertus, IT Dad, I/Watch, JClass, Jint, JProbe, LeccoTech, LiteSpeed, LiveReorg, MessageStats, NBSpool, NetBase, Npulse, NetPro, PassGo, PerformaSure, Quest Central, SharePlex, Sitraka, SmartAlarm, Spotlight, SQL LiteSpeed, SQL Navigator, SQL Watch, SQLab, Stat, StealthCollect, Tag and Follow, Toad, T.O.A.D., Toad World, vAnalyzer, vAutomator, vControl, vConverter, vEssentials, vFoglight, vMigrator, vOptimizer Pro, vPackager, vRanger, vRanger Pro, vReplicator, vSpotlight, vToad, Vintela, Virtual DBA, VizionCore, Vizioncore vAutomation Suite, Vizioncore vEssentials, Xaffire und XRT sind Warenzeichen oder eingetragene Warenzeichen von Quest Software, Inc. in den Vereinigten Staaten von Amerika und in anderen Ländern. Andere in diesem Handbuch aufgeführte Warenzeichen oder eingetragene Warenzeichen sind Eigentum ihrer jeweiligen Besitzer.

Haftungsausschluss

Die Informationen in diesem Dokument werden in Verbindung mit Quest-Produkten zur Verfügung gestellt. Durch dieses Dokument wird weder explizit noch implizit, durch Duldungsvollmacht oder auf andere Weise, eine Lizenz auf intellektuelle Eigentumsrechte erteilt, auch nicht in Verbindung mit dem Erwerb von Quest-Produkten. **MIT AUSNAHME DER BESTIMMUNGEN IN DEN ALLGEMEINEN GESCHÄFTSBEDINGUNGEN VON QUEST, DIE IN DER LIZENZVEREINBARUNG FÜR DIESES PRODUKT AUFGEFÜHRT SIND, ÜBERNIMMT QUEST KEINERLEI HAFTUNG UND SCHLIESST JEDE EXPLIZITE, IMPLIZITE ODER GESETZLICHE GEWÄHRLEISTUNG FÜR SEINE PRODUKTE AUS, INSBESONDERE DIE IMPLIZITE GEWÄHRLEISTUNG DER MARKTFÄHIGKEIT, DER EIGNUNG ZU EINEM BESTIMMTEN ZWECK UND DIE GEWÄHRLEISTUNG DER NICHTVERLETZUNG VON RECHTEN. UNTER KEINEN UMSTÄNDEN HAFTET QUEST FÜR UNMITTELBARE, MITTELBARE ODER FOLGESCHÄDEN, SCHADENERSATZ, BESONDERE ODER KONKRETE SCHÄDEN (INSBESONDERE SCHÄDEN, DIE AUS ENTGANGENEN GEWINNEN, GESCHÄFTSUNTERBRECHUNGEN ODER DATENVERLUSTEN ENTSTEHEN), DIE SICH DURCH DIE NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DIESES DOKUMENTS ERGEBEN, AUCH WENN QUEST ÜBER DIE MÖGLICHKEIT SOLCHER SCHÄDEN INFORMIERT WURDE.** Quest übernimmt keine Garantie für die Richtigkeit oder Vollständigkeit der Inhalte dieses Dokuments und behält sich vor, jederzeit und ohne vorherige Ankündigung Änderungen an den Spezifikationen und Produktbeschreibungen vorzunehmen. Quest geht keinerlei Verpflichtung ein, die in diesem Dokument enthaltenen Informationen zu aktualisieren.

Quest ActiveRoles Server – Administratorhandbuch
Aktualisiert – Oktober 14, 2009
Softwareversion – 6.5

INHALT

ÜBER DIESES HANDBUCH 11
ZIELGRUPPE DIESES HANDBUCHS 12
FORMATIERUNGSKONVENTIONEN 12
ÜBER QUEST SOFTWARE, INC. 13
KONTAKT ZU QUEST SOFTWARE 13
KONTAKT ZUM QUEST SUPPORT 13
EINLEITUNG 14

KAPITEL 1
ÜBER ACTIVEROLES SERVER 15
ZIELSETZUNG VON ACTIVEROLES SERVER 16
FUNKTIONEN VON ACTIVEROLES SERVER 17
DURCHSETZUNG VON UNTERNEHMENSRICHTLINIEN 17
AUTOMATISIERTE KONTOBEREITSTELLUNG 17
ROLLENBASIERTE VERTEILTE VERWALTUNG 18
WEITERGABE DELEGIERTER RECHTE AN ACTIVE DIRECTORY 18
SICHERHEITSVERWALTUNG FÜR ACTIVE DIRECTORY. 18
REGELORIENTIERTE ADMINISTRATIVE ANSICHTEN (VERWALTETE EINHEITEN) . . . 19
REGELORIENTIERTE GRUPPEN (DYNAMISCHE GRUPPEN) 19
REGELORIENTIERTE GRUPPENFAMILIEN 19
GENEHMIGUNGS-ARBEITSABLAUF 19
ERWEITERTE BERICHTERSTATTUNG. 20
NUTZEN VON ACTIVEROLES SERVER. 20
AUTOMATISIERTE BEREITSTELLUNG FÜR BENUTZER 20
VEREINFACHTE VERWALTUNG 21
VERBESSERTE SICHERHEIT 21
ERHÖHTE PRODUKTIVITÄT 22
TECHNISCHE ÜBERSICHT. 23
PRÄSENTATIONSKOMPONENTEN 24
DIENSTKOMPONENTEN 25
NETZWERKDATENQUELLEN 26
SICHERHEITS- UND VERWALTUNGSELEMENTE 27
SICHERHEITSVERWALTUNG FÜR ACTIVE DIRECTORY. 30
ADSI-PROVIDER UND SKRIPTRICHTLINIE ZUR UNTERSTÜTZUNG DER ANPASSUNG 31
DYNAMISCHE GRUPPEN 33
BETRIEB IN UMGEBUNGEN MIT MEHREREN GESAMTSTRUKTUREN 34

KAPITEL 2
ERSTE SCHRITTE 37
STARTEN DER ACTIVEROLES SERVER-KONSOLE 38
AUFRUFEN UND VERWENDEN DER HILFE 38
ÜBERBLICK ÜBER DIE BENUTZERSCHNITTSTELLE 39
KONSOLENSTRUKTUR 40
BEREICH „DETAILS" 40
BEREICH „ERWEITERT" 40
ANSICHTSMODUS 42
KONTROLLIERTE OBJEKTE 42
VERWENDEN VERWALTETER EINHEITEN 43
EINRICHTEN EINES FILTERS 44
SUCHEN NACH OBJEKTEN 44
ABRUFEN RICHTLINIENBEZOGENER INFORMATIONEN 46

KAPITEL 3
REGELBASIERTE ADMINISTRATIVE ANSICHTEN 49
VERWALTETE EINHEITEN 50
FUNKTIONSWEISE VERWALTETER EINHEITEN 50
ADMINISTRATION VERWALTETER EINHEITEN 51
ERSTELLEN EINER VERWALTETEN EINHEIT 51
ANZEIGEN DER MITGLIEDER EINER VERWALTETEN EINHEIT 56
HINZUFÜGEN UND ENTFERNEN VON MITGLIEDERN EINER VERWALTETEN EINHEIT 57
KOPIEREN EINER VERWALTETEN EINHEIT 58
EXPORTIEREN UND IMPORTIEREN EINER VERWALTETEN EINHEIT 58
UMBENENNEN EINER VERWALTETEN EINHEIT 58
LÖSCHEN EINER VERWALTETEN EINHEIT 59
SZENARIO: IMPLEMENTIEREN DER ROLLENBASIERTEN VERWALTUNG ÜBER MEHRERE ORGANISATIONSEINHEITEN HINWEG 59
SCHRITT 1: ERSTELLEN DER VERWALTETEN EINHEIT 60
SCHRITT 2: HINZUFÜGEN VON BENUTZERN ZU DER VERWALTETEN EINHEIT . . . 60
SCHRITT 3: VORBEREITEN DER ZUGRIFFSVORLAGE 60
SCHRITT 4: ANWENDEN DER ZUGRIFFSVORLAGE 60

KAPITEL 4
ROLLENBASIERTE ADMINISTRATION 61
ZUGRIFFSVORLAGEN ZUM DEFINIEREN VON ADMINISTRATORFUNKTIONEN 62
FUNKTIONSWEISE VON ZUGRIFFSVORLAGEN 62
SICHERHEITSSYNCHRONISIERUNG 63
VERWALTUNGSAUFGABEN FÜR ZUGRIFFSVORLAGEN 64
VERWENDEN VORDEFINIERTER ZUGRIFFSVORLAGEN 65
ERSTELLEN EINER ZUGRIFFSVORLAGE 68

Anwenden von Zugriffsvorlagen 76
Verwalten von Zugriffsvorlagenverknüpfungen. 79
Synchronisieren von Berechtigungen nach Active Directory 82
Hinzufügen, Ändern und Entfernen von Berechtigungen 86
Schachteln von Zugriffsvorlagen 87
Kopieren einer Zugriffsvorlage. 89
Exportieren und Importieren von Zugriffsvorlagen 89
Umbenennen einer Zugriffsvorlage 90
Löschen einer Zugriffsvorlage 90
Verwendungsbeispiele 90
Szenario 1: Implementieren eines Help Desk 90
Szenario 2: Implementieren der Selbstverwaltung 92

Kapitel 5
Regelbasierte automatische Bereitstellung und Deprovisionierung 95
Richtlinienobjekte. 96
Bereitstellungsrichtlinienobjekte 97
Deprovisionsrichtlinienobjekte 99
Funktionsweise von Richtlinienobjekten 100
Verwaltungsaufgaben für Richtlinienobjekte 101
Erstellen eines Richtlinienobjekts. 102
Hinzufügen, Ändern und Entfernen von Richtlinien 103
Anwenden von Richtlinienobjekten. 104
Verwalten des Richtlinienbereichs 107
Kopieren eines Richtlinienobjekts 113
Exportieren und Importieren von Richtlinienobjekten. 114
Umbenennen eines Richtlinienobjekts 114
Löschen eines Richtlinienobjekts. 114
Konfigurationsaufgaben für Richtlinien. 115
Erzeugung und Validierung von Eigenschaften 115
Erzeugung von Benutzeranmeldenamen 131
Automatische Bereitstellung der Gruppenmitgliedschaft 141
E-Mail-Aliaserzeugung 147
Automatische Bereitstellung von Exchange-Postfächern 152
Automatische Bereitstellung des Stammordners 156
Skriptausführung 166
Benutzerkontodeprovisionierung 172
Entfernen der Gruppenmitgliedschaft 183
Deprovisionierung des Exchange-Postfachs 188
Stammordner-Deprovisionierung 191
Benutzerkonto-Verschiebung 195

Permanentes Löschen von Benutzerkonten 197
Gruppenobjekt-Deprovisionierung 201
Gruppenobjekt-Verschiebung. 209
Dauerhaftes Löschen des Gruppenobjekts 211
Benachrichtigungsverteilung 214
Berichtsverteilung 220
Überprüfen der Richtlinieneinhaltung 224
Deprovisionieren von Benutzern oder Gruppen 227
Standardoptionen für die Deprovision 227
Delegieren der Deprovisionsaufgabe 229
Verwenden des Deprovisionsbefehls 230
Bericht zu Ergebnissen der Deprovision. 231
Wiederherstellen von deprovisionierten Benutzern oder Gruppen 238
Richtlinienoptionen für die Aufhebung der Deprovisionierung eines Benutzers 239
Delegieren der Aufhebung der Deprovision. 240
Verwenden des Befehls zur Aufhebung der Deprovision 241
Bericht über die Ergebnisse der Aufhebung der Deprovisionierung . . . 242
Richtlinie zur Vermeidung einer Containerlöschung 246
Erweiterungsfähigkeit von Richtlinien. 248
Designelemente 248
Erstellen und Verwalten von benutzerdefinierten Richtlinientypen. . . 250

Kapitel 6
Bestätigungsprüfung. 257
Beschreibung der Bestätigungsprüfung 258
Konfigurieren der Bestätigungsprüfung. 260
Starten oder Planen einer Prüfung 264
Durchführen der Bestätigung. 265
Untersuchen der Ergebnisse. 266
Untersuchen der Ergebnisse einer laufenden Prüfung 267
Untersuchen von historischen Ergebnissen 268
Delegieren von Bestätigungsprüfungsaufgaben 269

Kapitel 7
Arbeitsabläufe. 273
Beschreibung der Arbeitsabläufe. 274
Wichtige Funktionsmerkmale und Definitionen 274
Arbeitsablaufprozesse 276
Übersicht über die Arbeitsablaufaktivitäten 277
Übersicht über die Arbeitsablaufverarbeitung. 280

Konfigurieren eines Arbeitsablaufs 282
Erstellen einer Arbeitsablaufdefinition 283
Konfigurieren der Startbedingungen für einen Arbeitsablauf 283
Hinzufügen von Aktivitäten zu einem Arbeitsablauf 286
Konfigurieren einer Skriptaktivität 287
Konfigurieren einer Genehmigungsaktivität 288
Konfigurieren einer Benachrichtigungsaktivität 289
Konfigurieren einer Wenn-Dann-Sonst-Aktivität 291
Konfigurieren einer Stoppen/Unterbrechen-Aktivität 294
Aktivieren oder Deaktivieren eines Arbeitsablaufs 294
Beispiel: Genehmigungs-Arbeitsablauf 295
Begriffsdefinition 296
Funktionsweise 297
Erstellen und Konfigurieren eines Genehmigungs-Arbeitsablaufs . . 301

Kapitel 8
Temporäre Gruppenmitgliedschaft 305
Beschreibung von temporären Gruppenmitgliedschaften 306
Verwenden von temporären Gruppenmitgliedschaften 309
Hinzufügen von temporären Mitgliedern 309
Anzeigen von temporären Mitgliedern 310
Neuplanen von temporären Gruppenmitgliedschaften 311
Entfernen von temporären Mitgliedern 312

Kapitel 9
Gruppenfamilie 313
Grundlegendes zu Gruppenfamilien 314
Entwurfsübersicht 314
Funktionsweise 315
Erstellen einer Gruppenfamilie 317
Starten des Assistent für neue Gruppenfamilie 317
Name der Gruppenfamilie 318
Gruppierungsoptionen 319
Ort der verwalteten Objekte 320
Auswahl der verwalteten Objekte 321
Gruppieren-nach-Eigenschaften 323
Vorhandene Gruppen manuell erfassen 324
Gruppenbenennungsregel 325
Gruppenbereich und -typ 328
Ort der Gruppen 329
Exchange-bezogene Einstellungen 330
Planung für Gruppenfamilie 331

Verwalten einer Gruppenfamilie 332
Kontrollierte Gruppen 333
Registerkarte „Kontrollierte Gruppen“ 335
Registerkarte „Gruppierungen“ 338
Registerkarte „Zeitplan“ 339
Registerkarte „Vorgangsübersicht“ 340
Szenario: Abteilungsbezogene Gruppenfamilie 341

Kapitel 10
Dynamische Gruppen 343
Grundlegendes zu dynamischen Gruppen 344
Richtlinie zu dynamischen Gruppen 345
Verwalten dynamischer Gruppen 346
Konvertieren einer Standardgruppe in eine dynamische Gruppe 346
Anzeigen der Mitglieder einer dynamischen Gruppe 348
Hinzufügen einer Mitgliedschaftsregel zu einer dynamischen Gruppe 349
Entfernen einer Mitgliedschaftsregel aus einer dynamischen Gruppe 349
Konvertieren einer dynamischen Gruppe in eine Standardgruppe 349
Ändern, Löschen und Umbenennen einer dynamischen Gruppe 350
Szenario: Automatisches Verschieben von Benutzern zwischen Gruppen . . 350

Kapitel 11
ActiveRoles Server-Berichterstattung 353
Einleitung 354
Datenvorbereitungs-Collector für Berichte 355
Sammeln von Daten aus dem Netzwerk 357
Verarbeiten gesammelter Ereignisse 362
Quest Knowledge Portal für die Anzeige von Berichten 363
Arbeiten mit Berichten 364

Kapitel 12
Verwaltungsverlauf 371
Beschreibung des Verwaltungsverlaufs 372
Überlegungen und optimale Vorgehensweisen 372
Konfiguration des Verwaltungsverlaufs 375
Richtlinie für die Änderungsnachverfolgung 376
Konfiguration des Änderungsverfolgungsprotokolls 377
Replikation von Verwaltungsverlaufsdaten 378
Zentralisierte Verwaltungsverlaufsspeicherung 380
Untersuchen des Änderungsverlaufs 385
Untersuchen von Benutzeraktivitäten 387

KAPITEL 13
PAPIERKORB 389
BESCHREIBUNG DER PAPIERKORBFUNKTION 390
SUCHEN UND AUFLISTEN GELÖSCHTER OBJEKTE 390
SUCHEN NACH DEM CONTAINER „GELÖSCHTE OBJEKTE" 391
SUCHEN NACH OBJEKTEN, DIE AUS EINER BESTIMMTEN ORGANISATIONSEINHEIT ODER VERWALTETEN EINHEIT GELÖSCHT WURDEN . . 391
WIEDERHERSTELLEN EINES GELÖSCHTEN OBJEKTS 392
DELEGIEREN VON VORGÄNGEN AN GELÖSCHTEN OBJEKTEN 393
ANWENDEN VON RICHTLINIEN- ODER ARBEITSABLAUFREGELN 395

KAPITEL 14
AD LDS-DATENVERWALTUNG 397
REGISTRIEREN EINER AD LDS-INSTANZ 398
VERWALTEN VON AD LDS-OBJEKTEN 399
HINZUFÜGEN EINES AD LDS-BENUTZERS ZUM VERZEICHNIS 400
HINZUFÜGEN EINER AD LDS-GRUPPE ZUM VERZEICHNIS 401
HINZUFÜGEN ODER ENTFERNEN VON MITGLIEDERN ZU BZW. AUS EINER AD LDS-GRUPPE 401
DEAKTIVIEREN ODER AKTIVIEREN EINES AD LDS-BENUTZERKONTOS 402
FESTLEGEN ODER ÄNDERN DES KENNWORTS EINES AD LDS-BENUTZERS . . . 402
HINZUFÜGEN EINER ORGANISATIONSEINHEIT ZUM VERZEICHNIS 403
HINZUFÜGEN EINES AD LDS (ADAM)-PROXYOBJEKTS (BENUTZERPROXY) . . 404
ANPASSEN DER KONFIGURATION VON ACTIVEROLES SERVER 405
KONFIGURIEREN VON VERWALTETE EINHEITEN FÜR DIE AUFNAHME VON AD LDS-OBJEKTEN 405
ANZEIGEN ODER FESTLEGEN VON BERECHTIGUNGEN FÜR AD LDS-OBJEKTE . . 407
ANZEIGEN ODER FESTLEGEN VON RICHTLINIEN FÜR AD LDS-OBJEKTE 408

KAPITEL 15
VERWALTEN DER KONFIGURATION VON ACTIVEROLES SERVER 411
EINLEITUNG 412
HERSTELLEN EINER VERBINDUNG ZUM VERWALTUNGSDIENST 412
HINZUFÜGEN UND ENTFERNEN VERWALTETER DOMÄNEN 414
KONFIGURIEREN DER REPLIKATION 415
GRUNDLEGENDES ZUM REPLIKATIONSMODELL 415
KONFIGURIEREN VON SQL SERVER 417
ERSTELLEN EINER REPLIKATIONSGRUPPE 417
HINZUFÜGEN VON MITGLIEDERN ZU EINER REPLIKATIONSGRUPPE 418
ENTFERNEN VON MITGLIEDERN AUS EINER REPLIKATIONSGRUPPE 419
ÜBERWACHUNG DER REPLIKATION 420
VERWENDEN DER DATENBANKSPIEGELUNG 421
EINRICHTUNG DER DATENBANKSPIEGELUNG IN ACTIVEROLES SERVER 422

Erstellen und Verwenden virtueller Attribute 423
Szenario: Implementieren eines Attributs für den Geburtstag 424
Untersuchen von Client-Sitzungen 426
Überwachen der Leistung 427
Anpassen der Konsole 428
Seite „Andere Eigenschaften" im Objekterstellungsassistent 428
Registerkarte „Andere Eigenschaften" im Dialogfeld „Eigenschaften" 430
Anpassen von Anzeigenamen 431

Kapitel 16
Anhang 433
Anhang A: Verwenden regulärer Ausdrücke 434
Rangfolge 436
Anhang B: Administrative Vorlage für die ActiveRoles Server-Konsole . . 437
Installationsanweisungen 439

Über dieses Handbuch

- Zielgruppe dieses Handbuchs
- Formatierungskonventionen
- Über Quest Software, Inc.
- Kontakt zu Quest Software
- Kontakt zum Quest Support
- Einleitung

Zielgruppe dieses Handbuchs

Dieses Dokument wurde erstellt, um Sie mit Quest ActiveRoles Server vertraut zu machen. Das Administratorhandbuch enthält die erforderlichen Informationen zur Installation und Verwendung von Quest ActiveRoles Server. Es wurde als Nachschlagewerk für Netzwerkadministratoren, Berater, Analysten und andere IT-Fachleute entwickelt.

Formatierungskonventionen

In diesem Handbuch werden bestimmte Formatierungskonventionen eingehalten, die die effektive Verwendung des Dokuments sicherstellen. Diese Konventionen werden auf unterschiedliche Vorgänge, Symbole, Tastenkombinationen und Querverweise angewandt.

ELEMENT	KONVENTION
Auswählen	Dieses Wort bezieht sich auf Vorgänge wie das Auswählen oder Markieren diverser Benutzeroberflächenelemente wie zum Beispiel Dateien und Optionsfelder.
Fettdruck	In Quest Software-Produkten angezeigte Benutzeroberflächenelemente wie zum Beispiel Menüs und Befehle.
Kursivdruck	Wird für Anmerkungen verwendet.
Fetter Kursivdruck	Wird zur Hervorhebung verwendet.
Blaue Schrift	Zeigt einen Querverweis an. Kann in Adobe® Reader® als Hyperlink verwendet werden.
	Wird zum Hervorheben zusätzlicher Informationen verwendet, die für den jeweils beschriebenen Vorgang sachdienlich sind.
	Wird für empfohlene Vorgehensweisen verwendet. Eine empfohlene Vorgehensweise beschreibt einen Ablauf von Vorgängen detailliert, um optimale Ergebnisse zu erzielen.
	Damit werden Vorgänge hervorgehoben, die mit Vorsicht durchzuführen sind.
+	Ein Pluszeichen zwischen zwei Tasten bedeutet, dass beide Tasten gleichzeitig gedrückt werden müssen.
|	Ein senkrechter Strich zwischen Elementen bedeutet, dass Sie die Elemente in genau der angegebenen Reihenfolge auswählen müssen.

Über Quest Software, Inc.

Quest Software, Inc., bereits zweimal mit dem Titel „Global Independent Software Vendor Partner of the Year" der Microsoft Corporation ausgezeichnet, bietet innovative Produkte, die Unternehmen dabei unterstützen, die Leistung und Produktivität ihrer Anwendungen, Datenbanken, Windows-Infrastruktur und virtuellen Umgebungen zu steigern. Dank seines tiefgreifenden Know-hows im IT-Bereich und einer permanenten Konzentration auf bewährte Verfahren unterstützt Quest weltweit mehr als 100.000 Kunden dabei, die hohen Erwartungen an die Informationstechnologie ihrer Unternehmen zu erfüllen. Die Windows Managementlösungen von Quest vereinfachen, automatisieren, schützen und erweitern Active Directory, Exchange Server, SharePoint, SQL Server, .NET und Windows Server und integrieren Unix, Linux und Java in die verwaltete Umgebung. Software von Quest erhalten Sie in den weltweiten Niederlassungen und unter www.quest.com.

Kontakt zu Quest Software

E-Mail	info@quest.com
Postanschrift	Quest Software, Inc. World Headquarters 5 Polaris Way Aliso Viejo, CA 92656 USA
Website	www.quest.com

Informationen über unsere lokalen und internationalen Büros finden Sie auf unserer Website.

Kontakt zum Quest Support

Quest Support ist für Kunden verfügbar, die über eine Evaluierungsversion eines Quest-Produkts verfügen oder die eine handelsübliche Version erworben haben und über einen gültigen Wartungsvertrag verfügen. Der Quest-Support steht Ihnen über SupportLink, unsere Service-Website, rund um die Uhr zur Verfügung. Besuchen Sie SupportLink unter http://support.quest.com/.

Auf der SupportLink-Website stehen Ihnen folgende Funktionen zur Verfügung:

- Schnell Tausende von Lösungen finden (Knowledge Base-Artikel und Dokumente).
- Download von Patches und Aktualisierungen.
- Anfordern von Hilfe durch einen Support-Techniker.
- Protokollieren und Aktualisieren Ihres Einzelfalls sowie Überprüfung des Status Ihres Vorgangs.

Eine ausführlichere Erläuterung zu den Support-Programmen und zu den Online-Diensten sowie Kontaktinformationen und Angaben zu Richtlinien und Verfahren finden Sie im ***Global Support Guide***. Dieses Handbuch ist verfügbar unter: http://support.quest.com/pdfs/Global Support Guide.pdf.

Hinweis: Dieses Dokument ist nur in Englisch verfügbar.

Einleitung

Das *ActiveRoles Server Administratorhandbuch* ist für Personen konzipiert, die für die Implementierung der Verwaltungsstruktur von ActiveRoles Server verantwortlich sind. Dieses Dokument bietet konzeptionelle Informationen zum Produkt und enthält systematische Vorgehensweisen für die Einrichtung einer sicheren, dezentralen Verwaltungsstruktur, die die Durchsetzung administrativer Richtlinien, die rollenbasierte Delegierung von Verwaltungsrechten und flexible administrative Ansichten kombiniert.

Das *ActiveRoles Server Administratorhandbuch* wird durch das *ActiveRoles Server Benutzerhandbuch* ergänzt, das Informationen über die Benutzerschnittstelle der ActiveRoles Server-Konsole sowie Anleitungen, die die delegierten Administratoren und Help Desk-Mitarbeiter bei der Durchführung ihrer alltäglichen Verwaltungstätigkeiten mittels der ActiveRoles Server-Konsole unterstützen sollen, enthält.

1

Über ActiveRoles Server

- Zielsetzung von ActiveRoles Server
- Funktionen von ActiveRoles Server
- Nutzen von ActiveRoles Server
- Technische Übersicht

Zielsetzung von ActiveRoles Server

Mit der Entwicklung von Unternehmensnetzwerken hin zu verteilten, auf Clientdiensten basierenden Infrastrukturen steigt die Notwendigkeit einer inkrementellen Verwaltung. Dies veranlasst Organisationen zur Vereinfachung von Verwaltungsaufgaben, zur Steigerung der Sicherheit und zur Reduzierung der Netzwerkkosten. ActiveRoles Server genügt diesen Ansprüchen durch folgende Funktionen:

- Die Fähigkeit, Geschäftsregeln und administrative Richtlinien zur Sicherung des Sicherheitsmodells durchzusetzen, genügt allen organisatorischen Anforderungen.
- Die Fähigkeit, Kontrolle basierend auf anpassbaren Administratorfunktionen zu delegieren. Dies vereinfacht die Verwaltung von Active Directory vom Zeitpunkt der Einrichtung an.
- Die Fähigkeit, Berechtigungen in ActiveRoles Server festzulegen und zu ändern sowie diese Änderungen automatisch an Active Directory weiterzugeben.
- Die Fähigkeit, flexible, regelorientierte administrative Ansichten einzurichten, die die Verwaltung Active Directory-basierter Unternehmen über geografische Grenzen sowie über die Hierarchie von Organisationseinheiten hinweg ermöglichen.
- Die Fähigkeit, Verwaltungs- und Bereitstellungsaufgaben zu automatisieren, die einen vordefinierten, bedingungsgesteuerten Workflow aufweisen. So wird die Produktivität von Administratoren erhöht, und kostspielige Fehler werden vermieden.
- Sichere Verwaltung von Active Directory-Daten (Benutzerkonten, Gruppen, Computerkonten etc.) durch Richtlinieneinschränkungen und Automatisierungsfunktionen, die das Verbleiben veralteter Daten im Verzeichnis verhindern.
- Automatisierte, regelorientierte Verwaltung von Sicherheits- und Verteilergruppen. Diese ermöglicht die automatische Auffüllung von Gruppen und erhöht somit die Genauigkeit und Zuverlässigkeit.
- Verwaltung und Bereitstellung von Exchange-Postfächern.
- Überprüfung der Benutzerverwaltung und erweiterte Berichterstattung. Ein umfangreiches Paket von Berichten für die Verwaltung von Active Directory und Exchange kann zur Überprüfung anhand der Änderungsnachverfolgung, für die Durchsetzung von Unternehmensrichtlinien sowie die Überwachung und Analyse von Active Directory verwendet werden.
- Einfach zu verwendende Benutzeroberflächen, um die Netzwerkverwaltung zu optimieren und den Verwaltungsaufwand sowie die Kosten zu reduzieren.

ActiveRoles Server baut auf dem Verwaltungs- und Sicherheitsmodell von Active Directory auf und ermöglicht IT-Managern sowie Administratoren auf hoher Ebene eine effiziente Definition und Verteilung von Administratorrechten auf der Grundlage organisatorischer Rollen. ActiveRoles Server schließt außerdem eine regelorientierte, automatisierte Bereitstellung anderer IT-Ressourcen ein, die die Verwaltung von Active Directory vereinfacht und verhindert, dass das Verzeichnis mit beschädigten oder inkonsistenten Daten aufgefüllt wird.

ActiveRoles Server stellt eine sichere verteilte Verwaltung auf der Grundlage von Unternehmensregeln und -rollen bereit. Dazu werden flexible Rollendefinitionen, die Durchsetzung von Geschäftsregeln, Hilfe bei der Automatisierung sowie eine granuläre Delegierung der Kontrolle über Verzeichnisobjekte kombiniert. Aufbauend auf dem Delegierungsmodell von Active Directory ergänzt das Produkt die Delegationsfunktionen von Active Directory und optimiert die Verwaltung von Delegierungseinstellungen durch Speichern und Anwenden von Rolleninformationen für Administratorfunktionen im Einklang mit Geschäftsregeln des Unternehmens.

ActiveRoles Server ist eng in die Funktionalität von Active Directory integriert. Indem das Produkt anpassbare Richtlinien zusammen mit Active Directory-kompatiblen Berechtigungen verwendet, ermöglicht es Administratoren, autorisierten Benutzern eine angemessene Ebene der Kontrolle über Netzwerkressourcen bereitzustellen und administrative Richtlinien einzurichten, die automatisch durchgesetzt und unternehmensweit weitergegeben werden.

Mit ActiveRoles Server können Organisationen ihre Netzwerke dynamisch so konfigurieren, dass sowohl eine zentrale als auch eine verteilte Verwaltung von Active Directory als Sammelpunkt der Konfiguration, Verwaltung und Sicherheit von Netzwerkressourcen eingerichtet wird.

Funktionen von ActiveRoles Server

ActiveRoles Server erleichtert die Konten- und Ressourcenverwaltung und -bereitstellung für Active Directory und Exchange. ActiveRoles Server unterstützt Folgendes:

- Durchsetzung von Unternehmensrichtlinien
- Automatisierte Kontobereitstellung
- Rollenbasierte verteilte Verwaltung
- Weitergabe delegierter Rechte an Active Directory
- Sicherheitsverwaltung für Active Directory
- Regelorientierte administrative Ansichten (verwaltete Einheiten)
- Regelbasierte Gruppen (dynamische Gruppen und Gruppenfamilien)
- Genehmigungs-Arbeitsablauf
- Erweiterte Berichterstattung

Durchsetzung von Unternehmensrichtlinien

Im Interesse einer sicheren, verteilten Verwaltung müssen administrative Aktionen durch Richtlinien eingeschränkt werden. ActiveRoles Server integriert zu diesem Zweck Geschäftsregeln und Verzeichnisaktualisierungen miteinander. Bei jeder Verzeichnisaktualisierung wird eine anpassbare Gruppe von Prozeduren und Richtlinien aufgerufen. Mit dieser Funktion von ActiveRoles Server werden die Integrität, Konsistenz und Vollständigkeit der Verzeichnisdaten sichergestellt. Zudem wird Organisationen die Verbesserung ihrer Netzwerksicherheit erleichtert.

Automatisierte Kontobereitstellung

ActiveRoles Server stellt umfangreiche Automatisierungsfunktionen für administrative Prozesse bereit. Das Programm ermöglicht die Durchsetzung von Geschäftsregeln durch Ausführung benutzerdefinierter Skripts und Programme vor oder nach bestimmten Tasks und ermöglicht die Verknüpfung mehrerer separater Tasks zu einem einzelnen Vorgang. Diese Möglichkeit, Verwaltungs- und Bereitstellungsaufgaben im Einklang mit Unternehmensrichtlinien zu automatisieren, ist eine der wertvollsten Funktionen von ActiveRoles Server.

Rollenbasierte verteilte Verwaltung

Active Directory ermöglicht das Delegieren der administrativen Kontrolle an die Unternehmenseinheiten, die den Zugriff auf bestimmte Verwaltungstasks benötigen. Die Verwaltung einzelner Delegierungseinstellungen ist jedoch zeitaufwändig und fehleranfällig. ActiveRoles Server konsolidiert Delegierungsanforderungen mit Hilfe von anpassbaren Administratorfunktionen (Vorlagen), die die geschäftlichen Anforderungen der jeweiligen Organisation erfüllen. Mit Hilfe von Administratorfunktionen erhöht ActiveRoles Server die Produktivität der Administratoren und erleichtert die Vermeidung teurer Fehler bei der Verwaltung von Delegierungseinstellungen.

Weitergabe delegierter Rechte an Active Directory

Die in ActiveRoles Server angegebenen Rechte für die rollenbasierte Delegierung können an Active Directory weitergegeben werden. Sobald das Weitergeben für die delegierten Berechtigungen festgelegt ist, bleiben sie auch dann synchronisiert, wenn Änderungen in ActiveRoles Server vorgenommen werden.

Diese Funktion von ActiveRoles Server verbessert die Sicherheit von Active Directory, da sie die Komplexität der Zugriffskontrollverwaltung von Active Directory mit Hilfe der rollenbasierten Delegierung vereinfacht und indem sie Ihnen ermöglicht, präziser und effizienter den Zugriff einzuschränken und die Sicherheit zu bewerten.

Die Möglichkeit, delegierte Rechte an Active Directory weiterzugeben, verbessert die Kontrolle über das Delegierungsmodell von Active Directory. Die entstehende Gruppe von Berechtigungen zeigt die jeweilige Berechtigungsquelle und ermöglicht Ihnen die Ausführung von Berechtigungsüberprüfungen ohne manuelle Analyse des Berechtigungsursprungs. Dies reduziert das Risiko, dass Fehler unterlaufen oder etwas aus Versehen weggelassen wird.

Sicherheitsverwaltung für Active Directory

Die ActiveRoles Server-Konsole erleichtert die Untersuchung und Verwaltung von Berechtigungseinträgen in Active Directory und zeigt die den Benutzern zugewiesenen Zugriffsrechte zusammen mit dem Gültigkeitsbereich ihres Zugriffs. Eine zentrale Ansicht der Berechtigungseinträge hilft bei der Analyse und Verwaltung von Berechtigungen in Active Directory. Für jeden Berechtigungseintrag wird in der Ansicht eine Reihe von Eintragseigenschaften einschließlich der Beschreibung, des Ursprungs und des Sicherheitsprinzipals der Berechtigung angezeigt. Zusätzliche Eigenschaften können angezeigt werden, und auf den Editor für die einheitliche Sicherheit kann vom Hauptfenster aus zugegriffen werden.

Auf der ActiveRoles Server-Konsole können Sie die Berechtigungen für ein Objekt anzeigen, indem Sie einfach auf das Objekt klicken. Die Berechtigungseinträge werden dann in einer zentralen Ansicht angezeigt. Dies erleichtert Administratoren das Überprüfen der Berechtigungen für sicherheitsrelevante Objekte und das Identifizieren möglicher Sicherheitsprobleme.

Regelorientierte administrative Ansichten (verwaltete Einheiten)

Regelorientierte administrative Ansichten (bezeichnet als verwaltete Einheiten) erleichtern das Anzeigen und Verwalten des Unternehmens, ohne dass die zugrunde liegenden Domänen- und Organisationseinheitsstrukturen verändert werden. Da sie dynamisch an Veränderungen im Unternehmen angepasst werden können, vereinfachen verwaltete Einheiten die Wartung von Geschäftsregeln erheblich. Die Verwendung von verwalteten Einheiten erleichtert die Überwindung der Beschränkungen, die starren Organisationsstrukturen innewohnen, und entspricht der Anforderung, die Verwaltung außerhalb der Grenzen von Organisationseinheit, Domäne und Gesamtstruktur auszuführen.

Regelorientierte Gruppen (dynamische Gruppen)

ActiveRoles Server ermöglicht es, Gruppenmitgliedschaftslisten automatisch aktuell zu halten, sodass Sie Mitglieder nicht manuell hinzufügen und entfernen müssen. Die regelorientierte Verwaltung von Mitgliedschaftslisten verringert die Wartungskosten für Gruppen. Außerdem erhöht sie die Genauigkeit und Zuverlässigkeit der Nachrichtenverteilung über die Mitgliedschaft in Verteilergruppen sowie die Konsistenz von Sicherheitseinstellungen über die Mitgliedschaft in Sicherheitsgruppen.

Regelorientierte Gruppenfamilien

ActiveRoles Server stellt eine neue Kategorie regelorientierter Richtlinien für die automatische Gruppenbereitstellung bereit. Jede Richtlinie dieser Kategorie, die als Gruppenfamilie bezeichnet wird, dient als Kontrollmechanismus für die Erstellung und Auffüllung von Gruppen. Diese neuen Richtlinien sollen die bei der Verwaltung der Gruppenmitgliedschaft auftretenden Probleme lösen.

Die Gruppenfamilie erstellt automatisch Gruppen und pflegt Gruppenmitgliedschaftslisten. Dabei hält sie konfigurierbare Regeln ein. Die Gruppenmitgliedschaft kann somit anhand von Objekteigenschaften im Verzeichnis definiert werden. Die Gruppenfamilie ermöglicht außerdem die Erstellung neuer Gruppen anhand neuer Werte, die in Objekteigenschaften erkannt werden.

Die Konfiguration einer Gruppenfamilie muss nicht auf eine einzelne Objekteigenschaft beschränkt sein. Sie kann aus so vielen Eigenschaften kombiniert werden wie nötig. Beispielsweise kann eine Gruppenfamilie so eingerichtet werden, dass sie die Eigenschaften „Abteilung" und „Stadt" berücksichtigt. Folglich erstellt und pflegt die Gruppenfamilie eine separate Gruppe für jede Abteilung an jedem geografischen Standort.

Genehmigungs-Arbeitsablauf

ActiveRoles Server bietet in seinem Modul „Regeln & Rollen" Genehmigungs-Arbeitsablauffunktionen. Durch die Bereitstellung einer regelbasierten, anpassbaren Genehmigungsweiterleitung verringert ActiveRoles Server Fehler und Inkonsistenzen während der Verwaltung von Verzeichnisdaten. Während automatisierte Richtlinien keinen manuellen Eingriff erfordern, erweitert die auf Genehmigungen basierende Durchführung administrativer Vorgänge die Prozessautomatisierung um die Möglichkeit, angeforderte Vorgänge manuell zu genehmigen oder abzulehnen und die Ausführung von Genehmigungsaufgaben zu überwachen, um zu gewährleisten, dass diese zeitnah beantwortet werden.

Der Genehmigungs-Arbeitsablauf ist nützlich für eine Reihe von Benutzerverwaltungsaufgaben wie etwa die Erstellung, das Löschen und die Änderung von Objekten sowie die Bereitstellung und Deprovision von Benutzerkonten. Die Vorgänge können durch festgelegte Benutzer über das ActiveRoles Server Web-Interface initiiert werden.

Wenn ein angeforderter Vorgang die Berechtigung durch bestimmte Personen in einer Organisation erfordert, koordiniert ein Arbeitsablauf den Genehmigungsprozess. Das System führt den angeforderten Vorgang erst durch, wenn eine autorisierte Person die entsprechende Genehmigung erteilt hat.

Um den Genehmigungs-Arbeitsablauf zu konfigurieren, erstellt der Administrator Genehmigungsregeln mit Hilfe der ActiveRoles Server-Konsole. Genehmigungsregeln werden verwendet, um die Vorgänge anzugeben, die Gegenstand einer Genehmigung sind, und um die Personen festzulegen, die autorisiert sind, Genehmigungsaufgaben durchzuführen.

Erweiterte Berichterstattung

ActiveRoles Server verfügt über erweiterte Berichterstattungsfunktionen, mit denen alle administrativen Aktionen protokolliert und überprüft werden können. Das Berichterstattungspaket von ActiveRoles Server enthält zahlreiche vordefinierte Berichte, die alle möglichen administrativen Aktionen abdecken. Viele dieser Berichte sind anpassbar, sodass der Administrator den Berichtsinhalt steuern kann. Außerdem stellt ActiveRoles Server leicht zu verwendende Tools zum Erstellen beliebig vieler benutzerdefinierter Berichte bereit, in denen spezifische Daten wie beispielsweise der Zustands- und Änderungsverlauf eines Objekts isoliert dargestellt werden können.

Nutzen von ActiveRoles Server

Heute verlassen sich Organisationen zunehmend auf Active Directory und betrachten Active Directory als unternehmenswichtige Anwendung in ihrer Umgebung. Daher ist es wichtig, die mit Active Directory interagierenden Geschäftsprozesse zu steuern. Dies muss so sicher, so gut kontrolliert und so effizient wie möglich erfolgen. ActiveRoles Server ermöglicht die vollständige Steuerung der Verzeichnisverwaltung über die rollenbasierte Sicherheit und die regelorientierte Automatisierung der Tasks für die Bereitstellung, erneute Bereitstellung und Deprovision in Active Directory, Exchange und Windows. Das Programm bietet eine umfassende Lösung, die die Verwaltung vereinfacht, die Sicherheit verbessert und die Produktivität der Administratoren erhöht.

Automatisierte Bereitstellung für Benutzer

ActiveRoles Server automatisiert die Aufgaben der Bereitstellung für Benutzer, verringert so Ihre Arbeitslast für die Verwaltung und ermöglicht es, neuen Benutzern schneller die benötigten Ressourcen bereitzustellen. Das Programm automatisiert außerdem auch die erneute Bereitstellung und die Deprovision. Wenn der Zugriff eines Benutzers geändert oder entfernt werden muss, werden Aktualisierungen in Active Directory, Exchange und Windows also automatisch vorgenommen. Dies reduziert die Arbeitslast für die Verwaltung und ermöglicht Benutzern eine schnellere, größere Produktivität.

Vereinfachte Verwaltung

ActiveRoles Server ist einfach zu installieren, bereitzustellen und zu verwenden und ermöglicht den dafür ausgewählten Personen die schnelle und leichte Ausführung von Verwaltungsaufgaben. Dank der umfangreichen Integrationsfunktionen werden komplexe Aufgaben erleichtert und gegen Fehler abgesichert. Da administrative Richtlinien des Unternehmens durchgesetzt werden können, wird sichergestellt, dass der Sicherheitsentwurf und die Vorgehensweisen für den Betrieb unabhängig davon befolgt werden, welcher Administrator die Verwaltungsaufgaben ausführt. ActiveRoles Server vereinfacht die Verwaltung, sodass auch weniger umfassende Fähigkeiten ausreichen, um die Windows-Unternehmensinfrastruktur zu administrieren.

ActiveRoles Server stellt intuitiv verständliche, vereinheitlichte Benutzeroberflächen bereit, über die auch Mitarbeiter mit begrenzter Verwaltungserfahrung Netzwerkbenutzer, Gruppen und Computer verwalten können. Mit ActiveRoles Server können regelmäßige Verwaltungsaufgaben unter Wahrung der Sicherheit an abteilungsinterne Administratoren und an Help Desk-Operatoren delegiert werden, selbst wenn diese nur über grundlegendes Wissen verfügen.

Verbesserte Sicherheit

ActiveRoles Server ergänzt das Sicherheitsmodell von Active Directory und stellt sicher, dass die Genauigkeit der Verzeichnisdaten anhand administrativer Richtlinien des Unternehmens aufrechterhalten wird. Die Richtliniendurchsetzung dieses Produkts stellt sicher, dass jede administrative Aktion den Sicherheitsstandards des Unternehmens entspricht. Dies hat für die meisten Organisationen höchste Priorität.

Mit ActiveRoles Server können Verwaltungsaufgaben auf sichere Weise an die passenden Personen delegiert werden. Das Programm stellt eine richtlinienbasierte, kontrollierte Umgebung bereit, in der autorisierte Benutzer mit Verzeichnisdatenquellen interagieren können, und stellt konsistente Ebenen von Administratorrechten, eine verbesserte Sicherheit sowie eine vereinfachte Verwaltung der Verzeichnisdaten sicher.

Alle Aktivitäten von ActiveRoles Server werden in einem separaten Ereignisprotokoll aufgezeichnet. Diese detaillierten Protokolleinträge ermöglichen die schnelle Identifikation und Verwaltung potenzieller Sicherheitsprobleme. ActiveRoles Server stellt ein vollständiges Prüfprotokoll bereit. Dieses zeigt alle ausgeführten Aktionen und ihre Urheber sowie auch Aktionen, die nicht zugelassen wurden. Durch eine Analyse des Prüfprotokolls können Sie Sicherheitsbedrohungen erkennen und Sicherheitsprobleme verhindern.

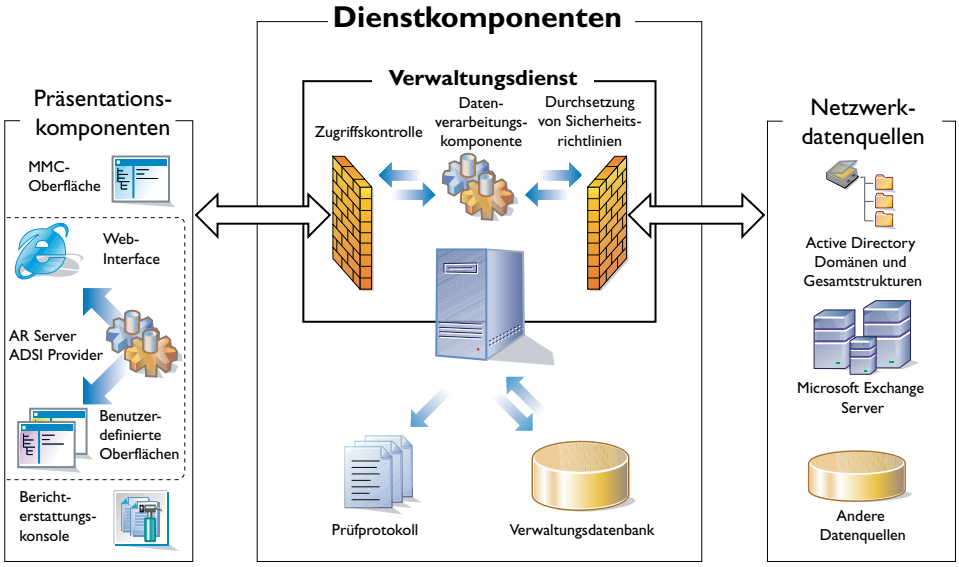
Erhöhte Produktivität

ActiveRoles Server erhöht die Produktivität der Verzeichnisadministratoren und Help Desk-Operatoren durch Automatisieren der Bereitstellungsaufgaben wie das Erstellen von Exchange-Postfächern, das Zuweisen von Stammordnern und das Warten von Gruppen. Ebenfalls vorhanden sind umfangreiche Skriptfunktionen, die eine flexible Automatisierungsmöglichkeit für Verwaltungsvorgänge bereitstellen und mit denen Active Directory und Exchange in andere Geschäftsprozesse integriert werden können. Dank der anpassbaren Integration und der Automatisierung von Verwaltungsaufgaben erhöht ActiveRoles Server die Produktivität und hilft bei der Vermeidung teurer Fehler.

Die von ActiveRoles Server bereitgestellte automatisierte Richtliniendurchsetzung stellt sicher, dass Unternehmensrichtlinien konsistent befolgt werden, unabhängig davon, welche Person administrative Aktionen ausführt. Durch die Verteilung und Automatisierung regelmäßiger Verwaltungsaufgaben ermöglicht ActiveRoles Server es Verzeichnisadministratoren, sich auf strategische Vorhaben wie die Planung des Verzeichnisses, die Erhöhung der Unternehmenssicherheit oder die Unterstützung unternehmenswichtiger Anwendungen zu konzentrieren.

Technische Übersicht

ActiveRoles Server teilt die Arbeitslast der Verzeichnisverwaltung und der Bereitstellung in drei Funktionsebenen auf: Präsentationskomponenten, Dienstkomponenten und Netzwerkdatenquellen.



Zu den Präsentationskomponenten gehören Clientbenutzeroberflächen für die Windows-Plattform und das Web, mit denen gewöhnliche Benutzer einen genau definierten Satz administrativer Aktionen ausführen können. Die Berichterstattungslösung erleichtert das automatisierte Generieren von Berichten zu Verwaltungsaktivitäten.

Die Dienstkomponenten stellen eine geschützte Ebene zwischen Administratoren und verwalteten Datenquellen dar. Diese Ebene stellt eine konsistente Durchsetzung von Richtlinien sicher, stellt erweiterte Automatisierungsfunktionen bereit und ermöglicht die Integration von Geschäftsprozessen für die Verwaltung von Active Directory, Microsoft Exchange und anderen Datenquellen im Unternehmen.

In der Verwaltungsdatenbank werden Informationen zu allen Berechtigungs- und Richtlinien-einstellungen sowie andere Daten im Zusammenhang mit der ActiveRoles Server-Konfiguration gespeichert.

Die Komponenten von ActiveRoles Server arbeiten auf einer sehr hohen Ebene wie folgt zusammen, um Verzeichnisdaten zu bearbeiten:

1. Ein Administrator greift über die MMC-Benutzeroberfläche oder das Web-Interface auf ActiveRoles Server zu.
2. Der Administrator übersendet eine Vorgangsanforderung, z.B. eine Abfrage oder eine Datenänderung, an den Verwaltungsdienst.
3. Bei Erhalt der Vorgangsanforderung überprüft der Verwaltungsdienst, ob der Administrator über hinreichende Berechtigungen zum Ausführen des angeforderten Vorgangs verfügt (Zugriffsprüfung).
4. Der Verwaltungsdienst stellt sicher, dass der angeforderte Vorgang die Unternehmensrichtlinien nicht verletzt (Richtliniendurchsetzung).
5. Der Verwaltungsdienst führt alle aufgrund von Unternehmensrichtlinien erforderlichen Aktionen aus, bevor er die Anforderung zur Verarbeitung freigibt (Richtliniendurchsetzung).

6. Der Verwaltungsdienst gibt Aufrufe von Betriebssystemfunktionen aus, um den angeforderten Vorgang für Netzwerkdatenquellen auszuführen.
7. Der Verwaltungsdienst führt nach der Verarbeitung der Anforderung durch das Betriebssystem alle zugehörigen Aktionen aus, die aufgrund der Unternehmensrichtlinien erforderlich sind (Richtliniendurchsetzung).
8. Der Verwaltungsdienst generiert ein Prüfprotokoll, das Datensätze zu allen mit ActiveRoles Server ausgeführten oder versuchten Vorgängen enthält. Nachverfolgungsberichte für Verzeichnisänderungen basieren auf dem Prüfprotokoll.

Im Folgenden werden die drei Komponentenebenen betrachtet.

Präsentationskomponenten

Zu den Präsentationskomponenten gehören Benutzeroberflächen, die eine Vielzahl von Anforderungen erfüllen. Die Benutzeroberfläche akzeptiert Befehle, zeigt Kommunikationsdaten an und präsentiert Ergebnisse auf klare, prägnante Weise.

ActiveRoles Server-Konsole (MMC-Schnittstelle)

Die ActiveRoles Server-Konsole, auch als MMC-Schnittstelle bezeichnet, ist ein umfassendes Verwaltungstool für Active Directory und Microsoft Exchange. Sie ermöglicht das Festlegen von Administratorfunktionen und das Delegieren der Kontrolle, das Definieren von administrativen Richtlinien und Automatisierungsskripts, das einfache Finden von Verzeichnisobjekten und die Ausführung von Verwaltungsaufgaben.

Web-Interface

Über das Web-Interface können Intranetbenutzer mit ausreichenden Administratorrechten eine Verbindung mit ActiveRoles Server herstellen, um grundlegende Verwaltungsaufgaben wie etwa die Änderung von Benutzerdaten oder das Hinzufügen von Benutzern zu Gruppen ausführen. Das Web-Interface stellt Mitarbeitern der Abteilungen und des Help Desk die Verwaltungsfunktionen bereit, die sie benötigen.

Benutzerdefinierte Benutzeroberflächen

Zusätzlich zur MMC-Benutzeroberfläche und zum Web-Interface ermöglicht ActiveRoles Server auch die Entwicklung benutzerdefinierter Benutzeroberflächen, die über den ADSI-Provider von ActiveRoles Server auf die Funktionen von ActiveRoles Server zugreifen. Administratoren mit Kenntnissen der Skripterstellung und Programmierung können benutzerdefinierte Benutzeroberflächen erstellen, die die spezifischen Anforderungen für die Netzwerkverwaltung erfüllen.

ADSI-Provider von ActiveRoles Server

Der ActiveRoles Server ADSI Provider wird als Teil der Darstellungskomponenten ausgeführt, um benutzerdefinierten Benutzerschnittstellen und Anwendungen den Zugriff auf Active Directory-Dienste über ActiveRoles Server zu ermöglichen. Der ActiveRoles Server ADSI Provider übersetzt die Anforderung der Clients in DCOM-Aufrufe und interagiert mit dem Verwaltungsdienst.

Der ActiveRoles Server ADSI Provider ermöglicht benutzerdefinierten Skripts und Anwendungen wie etwa webbasierten Anwendungen, mit Active Directory zu kommunizieren, während er gleichzeitig die Sicherheits-, Arbeitsablaufintegrations- und Berichterstattungsfunktionen von ActiveRoles Server nutzt. So können zum Beispiel bei Verwendung des ActiveRoles Server ADSI Provider webbasierte Seiten erstellt werden, sodass die von Help Desk-Mitarbeitern vorgenommenen Änderungen an den Benutzereigenschaften durch die von ActiveRoles Server erzwungenen Unternehmensregeln eingeschränkt werden.

Berichtslösung

ActiveRoles Server bietet eine umfassende Berichtslösung für die Überwachung von administrativen Vorgängen, der Einhaltung der Unternehmensrichtlinien und des Status von Verzeichnisobjekten. Die ActiveRoles Server Berichtslösung umfasst den Data Collector und das Report Pack.

Report Pack bietet Berichtsdefinitionen für die Erstellung von Berichten auf der Grundlage der vom Data Collector erfassten Daten. ActiveRoles Server enthält eine umfassende Sammlung von Berichtsdefinitionen, die alle in diesem Produkt verfügbaren Verwaltungsaktionen abdecken.

Report Pack erfordert Microsoft SQL Server Reporting Services (SSRS). Sie können die in SSRS enthaltenen Tools für die Anzeige, die Speicherung, den Druck, die Veröffentlichung und die Planung von ActiveRoles Server-Berichten nutzen.

Data Collector wird für die Erfassung der für die Berichterstattung erforderlichen Daten verwendet. Der Data Collector-Assistent ermöglicht Ihnen, Datenerfassungsaufträge zu konfigurieren und zu planen.

Nach Abschluss der Konfiguration fragt Data Collector Daten von verschiedenen Quellen ab, indem er über den ActiveRoles Server-Verwaltungsdienst auf diese Daten zugreift und sie dann in einer SQL Server-Datenbank speichert. Data Collector stellt außerdem ein Mittel für die Verwaltung der erfassten Daten dar und bietet darüber hinaus die Möglichkeit, veraltete Daten zu exportieren oder zu löschen.

Dienstkomponenten

Der Verwaltungsdienst bildet das Kernstück von ActiveRoles Server. Er enthält erweiterte Delegationsfunktionen und gewährleistet die zuverlässige Durchsetzung administrativer Richtlinien, mit denen Daten aktuell und genau gehalten werden. Der Verwaltungsdienst fungiert als eine Art Brücke zwischen den Präsentationskomponenten und den Netzwerk-Datenquellen. In großen Netzwerken können mehrere Verwaltungsdienste bereitgestellt werden, um die Leistung zu steigern und um eine Fehlertoleranz zu gewährleisten.

Datenverarbeitungskomponente

Die Datenverarbeitungskomponente akzeptiert administrative Anforderung und validiert sie, indem sie die in der Verwaltungsdatenbank gespeicherten Berechtigungen und Regeln überprüft. Diese Komponente verwaltet die Netzwerkdatenquellen. Anhand von administrativen Anforderungen und Richtliniendefinitionen ruft sie die entsprechenden Netzwerkobjektdaten ab oder ändert sie.

Die Datenverarbeitungskomponente fungiert als ein sicherer Dienst. Sie meldet sich mit Domänen-Benutzerkonten an, die über ausreichende Rechte für den Zugriff auf die Domänen verfügen, die bei ActiveRoles Server registriert sind (verwaltete Domänen). Der Zugriff auf die verwalteten Domänen wird durch die Zugriffsrechte dieser Benutzerkonten eingeschränkt.

Konfigurationsdatenbank

Der Verwaltungsdienst verwendet die Konfigurationsdatenbank (die auch als Verwaltungsdatenbank bezeichnet wird) für die Speicherung von Konfigurationsdaten. Die Konfigurationsdaten umfassen die Definition von ActiveRoles Server-spezifischen Objekten, die Zuweisungen von Administratorfunktionen und Richtlinien sowie die für die Durchsetzung der Richtlinien verwendeten Verfahren. Die Verwaltungsdatenbank wird nur für die Speicherung von ActiveRoles Server-Konfigurationsdaten verwendet. Sie speichert keine Kopien der Objekte, die sich in den verwalteten Datenquellen befinden, noch wird sie als ein Objektdaten-Zwischenspeicher verwendet.

ActiveRoles Server verwendet Microsoft SQL Server zum Hosten der Konfigurationsdatenbank. Die Replikationsfunktionen von SQL Server erleichtern die Implementierung von mehreren äquivalenten Konfigurationsdatenbanken, die von verschiedenen Verwaltungsdiensten verwendet werden.

Prüfprotokoll

Die Datenverarbeitungskomponente bietet einen umfassenden Audit Trail, indem sie Einträge im Ereignisprotokoll auf dem Computer erstellt, auf dem der Verwaltungsdienst ausgeführt wird. Das Protokoll zeigt alle ausgeführten Aktionen und ihre Urheber sowie Aktionen, die nicht zugelassen wurden. Die Protokolleinträge zeigen den Erfolg oder Fehler jeder Aktion sowie die geänderten Attribute an.

Netzwerkdatenquellen

Über den Verwaltungsdienst greift ActiveRoles Server auf die in den folgenden Datenquellen gespeicherten Objektdaten zu und steuert sie:

- **Active Directory-Domänen und Gesamtstrukturen** Stellt die Verzeichnisobjektinformationen in Active Directory-Domänen bereit.
- **Microsoft Exchange Server** Stellt Informationen zu Postfächern bereit, die von Microsoft Exchange verwaltet werden.
- **Andere Datenquellen** Stellt Informationen über außerhalb von Active Directory existierende Objekte bereit. Hierzu gehören Informationen aus Unternehmensdatenbanken wie etwa die Datenbank der Personalabteilung und Informationen über Computerressourcen wie etwa Dienste, Drucker und Netzwerkdateifreigaben.

ActiveRoles Server hilft bei der Verwendung und Verwaltung dieser Datenquellen. Verzeichnisadministratoren können Geschäftsregeln und Geschäftsrichtlinien definieren und durchsetzen, um sicherzustellen, dass die Daten in den verwalteten Datenquellen aktuell und genau bleiben.

Mit ActiveRoles Server können Sie die Informationsspeicher aus einer Vielzahl von Datenquellen im Netzwerk verwenden, z.B. Daten der Personalabteilung oder Inventardaten. Sie können die Skripterstellung für die Integration dieser wichtigen Datenquellen verwenden. Dies verringert doppelte Arbeiten und die Datenverfälschung und ermöglicht die Auswertung von Informationen, die häufig in mehr als einer Datenbank gespeichert werden.

ActiveRoles Server ermöglicht einem benutzerdefinierten Skript, auf Aufforderung die Kontrolle zu übernehmen, um einen administrativen Vorgang wie etwa die Objekterstellung, -änderung oder -löschung durchzuführen. Benutzerdefinierte Skripts können über Richtlinienobjekte aufgerufen werden, die ActiveRoles Server verwendet, um Unternehmensregeln durchzusetzen. So können Sie zum Beispiel ein Richtlinienobjekt implementieren, das ein benutzerdefiniertes Skript enthält, das immer dann die Kontrolle übernimmt, wenn ActiveRoles Server zur Erstellung eines Benutzerobjekts in einer bestimmten Organisationseinheit aufgefordert wird.

Das Richtlinienobjekt kann so konfiguriert werden, dass ActiveRoles Server die Erstellung des Benutzer nur nach erfolgreicher Ausführung eines bestimmten Abschnitt des Skripts fortsetzt (der vor der Erstellung eingesetzte Ereignis-Handler). Auf diese Weise verhindert das Skript die Erstellung von Benutzerobjekten, deren Eigenschaften gegen Unternehmensregeln verstoßen. Es verhindert das Füllen von Objekteigenschaften mit Werten, die aus externen Datenquellen stammen, und generiert Standard-Eigenschaftswerte in Übereinstimmung mit den Unternehmensregeln.

Das Richtlinienobjekt kann auch so konfiguriert werden, dass die Kontrolle unmittelbar nach erfolgreicher Erstellung eines Benutzerobjekts an einen anderen Teil des Skripts übergeben wird (der nach der Erstellung eingesetzte Ereignis-Handler). Dies ermöglicht dem Skript, zusätzliche, von Unternehmensregeln geforderte Vorgänge auszulösen, nachdem das Objekt erstellt wurde. So kann es zum Beispiel externe Datenspeicher aktualisieren, dem Benutzer einen Zugriff auf Ressourcen bereitstellen und über die Erstellung des Benutzerobjekts informieren.

Sicherheits- und Verwaltungselemente

ActiveRoles Server umfasst drei wichtige Sicherheits- und Verwaltungselemente, die als Objekte in der Verwaltungsdatenbank gespeichert sind:

- Zugriffsvorlagen
- Richtlinienobjekte
- Verwaltete Einheiten

Diese Elemente ermöglichen es, jedem Benutzer oder jeder Gruppe in Active Directory eingeschränkte und effektiv kontrollierte administrative Rechte zu gewähren.

Benutzer und Gruppen, denen administrative Berechtigungen in ActiveRoles Server eingeräumt werden, werden als *Trustees* bezeichnet. Trustees können verwalteten Einheiten oder Verzeichnisobjekten und Containern zugewiesen werden.

Trustees haben keine speziellen administrativen Rechte innerhalb von Active Directory. Um Trustees Zugriff auf Active Directory zu gewähren, implementiert ActiveRoles Server Proxy-Mechanismen, die Zugriffsvorlagen für die Festlegung der Zugriffsebene verwenden. Wenn Trustees ihre Zugriffs-berechtigungen wahrnehmen, verwenden diese Mechanismen Richtlinienobjekte für die Auslösung weiterer Vorgänge wie etwa die Ausführung von Integrationsskripts und die Validierung von Eingangsdaten.

Wenn Sie einen Benutzer oder eine Gruppe zu einem Trustee ernennen, müssen Sie die Zugriffsvorlagen angeben, die kontrollieren, zu welchen Vorgängen der Trustee berechtigt ist. Einer Gruppe gewährte Berechtigungen gelten für alle Mitglieder dieser Gruppe. Um den Verwaltungsaufwand zu reduzieren, sollte die administrative Kontrolle an Gruppen und nicht an einzelne Benutzer delegiert werden.

Um Richtlinieneinschränkungen und eine Automatisierung zu implementieren, müssen Sie Richtlinienobjekte konfigurieren und anwenden, die bei administrativen Anforderungen integrierte oder benutzerdefinierte Verfahren aufrufen. Richtlinienverfahren können die Ausführung von benutzerdefinierten Skripts für die Synchronisation von Active Directory-Daten mit anderen Datenquellen, die Durchführung einer Datengültigkeitsprüfung und den Start weiterer administrativer Vorgänge umfassen.

Zugriffsvorlagen für die rollenbasierte Administration

Eine *Zugriffsvorlage* ist eine Sammlung von Berechtigungen, die definieren, welche Vorgänge von einer administrativen Rolle ausgeführt werden können. ActiveRoles Server wendet Zugriffsvorlagen auf Verzeichnisobjekte, Container und administrative Ansichten (verwaltete Einheiten) an, die in Zusammenhang mit zu Trustees ernannten Gruppen und Benutzern stehen.

ActiveRoles Server bietet eine umfangreiche Suite vordefinierter Zugriffsvorlagen, die typische Administratorfunktionen darstellen und das schnelle und konsistente Delegieren der richtigen Administratorautoritätsebene ermöglichen. Zugriffsvorlagen vereinfachen in erheblichem Maß die Delegation und Verwaltung von administrativen Rechten, beschleunigen die Bereitstellung des Delegationsmodells und verringern die Verwaltungskosten. Die vorkonfigurierten Zugriffsvorlagen werden im Dokument *Sofort verwendbare ActiveRoles Server-Zugriffsvorlagen* beschrieben.

Zugriffsvorlagen ermöglichen zentralisierten Administratoren die Definition von Administratorfunktionen mit verschiedenen Berechtigungsebenen, wodurch die Bereitstellung einer Zugriffskontrolle beschleunigt und die Verfolgung von Änderungen an Berechtigungseinstellungen im gesamten Unternehmen rationalisiert wird.

Es ist auch möglich, benutzerdefinierte Zugriffsvorlagen auf der Grundlage von Businessanforderungen zu erstellen. Benutzerdefinierte Zugriffsvorlagen können jederzeit geändert werden. Wenn eine Zugriffsvorlage geändert wird, ändern sich die Berechtigungseinstellungen für alle Objekte, auf die diese Zugriffsvorlage angewandt wird, entsprechend.

Richtlinienobjekte zur Erzwingung von Unternehmensregeln

Ein *Richtlinienobjekt* ist eine Sammlung administrativer Richtliniendefinitionen, die durchzusetzende Unternehmensregeln angeben. Zugriffsvorlagen legen fest, wer Änderungen an Datensätzen vornehmen darf, und Richtlinienobjekte kontrollieren, welche Änderungen an den Daten vorgenommen werden dürfen. ActiveRoles Server setzt Unternehmensregeln durch Verknüpfen von Richtlinienobjekten mit folgenden Elementen um:

- Administrative Ansichten (verwaltete Einheiten)
- Active Directory-Container
- Individuelle Verzeichnisobjekte

Richtlinienobjekte definieren das Verhalten des Systems bei der Erstellung oder Änderung, beim Verschieben oder beim Löschen von Verzeichnisobjekten. Richtlinien werden unabhängig von den Berechtigungen eines Trustees erzwungen.

Ein Richtlinienobjekt schließt gespeicherte Richtlinienprozeduren und Angaben von Ereignissen ein, die die jeweilige Prozedur aktivieren. Auf der Grundlage von Richtlinienanforderungen kann ein Richtlinienverfahren folgende Aktionen durchführen:

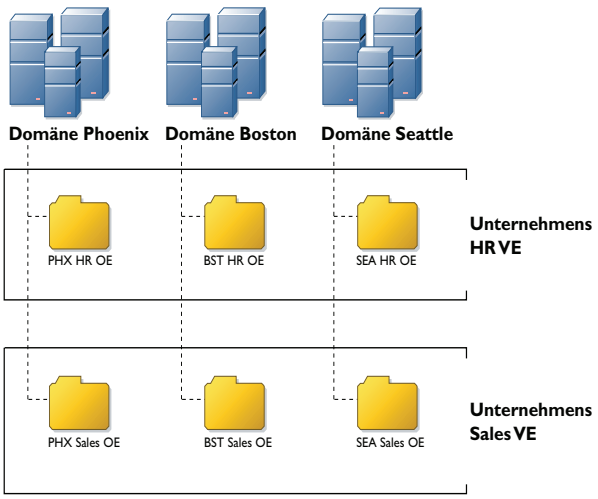
- Validieren von spezifischen Eigenschaftswerten
- Zulassen oder Verweigern von ganzen Vorgängen
- Auslösen weiterer Vorgänge

Ein Richtlinienobjekt ordnet seinen Richtlinienprozeduren spezifische Ereignisse zu, bei denen es sich um integrierte Prozeduren oder benutzerdefinierte Skripts handeln kann. Dies ermöglicht die einfache Implementierung komplexer Überprüfungskriterien, die Synchronisierung verschiedener Datenquellen und die Kombination einer Reihe von Verwaltungstasks in einem einzelnen Batch.

Verwaltete Einheiten für die Bereitstellung administrativer Ansichten

Eine *verwaltete Einheit* ist eine Sammlung von Objekten, die gemeinsam mit Hilfe von ActiveRoles Server verwaltet werden und die für die Verteilung von administrativen Verantwortlichkeiten, die Durchsetzung von Business-Regeln und Unternehmensstandards und die Verwaltung von komplexen Netzwerkumgebungen erstellt wurden. Mit Hilfe von verwalteten Einheiten kann das Verwaltungsgerüst vom Active Directory-Design getrennt werden. Verzeichnisobjekte können unabhängig vom Speicherort des Objekts in Active Directory einfach in administrativen Ansichten zusammengefasst werden.

So kann das Active Directory-Design zum Beispiel auf dem geografischen Standort beruhen, wobei Domänen nach Städten oder Regionen und Organisationseinheiten nach Unternehmensabteilungen oder -gruppen benannt werden. Verwaltete Einheiten können jedoch auch so gestaltet werden, dass spezifische Abteilungen oder Gruppen verwaltet werden, die auf mehrere geografische Standorte aufgeteilt sind.



In diesem Beispiel hat jede AD-Domäne eine „Human Resources" (HR) -Organisationseinheit und eine „Sales"-Organisationseinheit. Das ActiveRoles Server-Design hat eine verwaltete Einheit „HR" und eine verwaltete Einheit „Sales". Die verwaltete Einheit „HR" ermöglicht es den Administratoren, die für alle HR-Benutzer erforderlichen Richtlinien und Sicherheitseinschränkungen unabhängig von deren Standort zu konfigurieren, während die verwaltete Einheit „Sales" dieselbe Funktion für alle Sales-Benutzer bietet.

Verwaltete Einheiten werden mit Hilfe von Mitgliedschaftsregeln definiert. Hierbei handelt es sich um Kriterien, die von ActiveRoles Server verwendet werden, um zu ermitteln, ob ein Objekt zu einer bestimmten verwalteten Einheit gehört oder nicht. Dies ermöglicht die dynamische Änderung von verwalteten Einheiten, wenn sich die Netzwerkumgebung ändert. Sie können zum Beispiel eine verwaltete Einheit definieren, indem Sie Regeln angeben, die alle Objekte umfassen, deren Eigenschaften mit bestimmten Bedingungen übereinstimmen. Die angegebenen Regeln zwingen die neuen oder geänderten Objekte, Mitglieder der richtigen verwalteten Einheit zu sein.

Verwaltete Einheiten erweitern die Funktion von Organisationseinheiten, indem Sie einen bequemen Bereich für die Delegation der Verwaltung und die Erzwingung von Unternehmensregeln bieten. Eine verwaltete Einheit weist die folgenden Merkmale auf:

- Sie stellt eine Sammlung von Objekten dar (ein Objekt kann zu mehr als einer verwalteten Einheit gehören)
- Sie unterstützt regelbasierte Spezifikationen für ihre Mitglieder (eine verwaltete Einheit enthält nur Objekte, die den für die verwaltete Einheit angegebenen Mitgliedschaftsregeln entsprechen)
- Sie kann Verzeichnisobjekte enthalten, die sich in verschiedenen Organisationseinheiten, Domänen, Gesamtstrukturen und anderen verwalteten Einheiten befinden

ActiveRoles Server stellt sicher, dass für eine verwaltete Einheit angegebene Berechtigungs- und Richtlinieneinstellungen von allen Objekten, die zu dieser verwalteten Einheit gehören, übernommen werden. Wenn ein Verzeichniscontainer zu einer verwalteten Einheit gehört, erben alle untergeordneten Objekte in diesem Container die auf der Ebene der verwalteten Einheit definierten Berechtigungs- und Richtlinieneinstellungen. Diese Vererbung setzt sich die gesamte Verzeichnisstruktur innerhalb aller Containerobjekte, die Mitglieder der verwalteten Einheit sind, nach unten fort.

Sicherheitsverwaltung für Active Directory

Die ActiveRoles Server MMC-Schnittstelle erleichtert die Untersuchung und Verwaltung von Berechtigungseinträgen in Active Directory, indem sie den für jeden Benutzer verfügbaren Zugriff zusammen mit dem Gültigkeitsbereich ihres Zugriffs anzeigt. Eine zentrale Ansicht aller Berechtigungseinträge für ein bestimmtes Objekt hilft bei der Analyse und Verwaltung von Berechtigungen in Active Directory. Für jeden Berechtigungseintrag wird in der Ansicht eine Reihe von Eintragseigenschaften einschließlich der Beschreibung, des Ursprungs und des Sicherheitsprinzipals der Berechtigung angezeigt. Ausgehend vom Hauptfenster können Zusätzliche Eigenschaften angezeigt werden. Außerdem kann auf den Editor für die einheitliche Sicherheit zugegriffen werden.

Die zentralisierte Anzeige der einheitlichen Sicherheit ermöglicht es dem Administrator, schnell die Berechtigungen einzusehen, die Objekten in Active Directory zugewiesen sind, und zu ermitteln, ob die Berechtigung übernommen wurde oder nicht. Die Liste der Berechtigungseinträge kann nach dem Sicherheitsprinzipalnamen sortiert werden, um zu ermitteln, wer Zugriff auf das ausgewählte Objekt hat. Wenn ein Berechtigungseintrag übernommen wurde, gibt ActiveRoles Server das Objekt an, von dem die Berechtigung stammt, sodass der Administrator den Berechtigungseintrag für dieses Objekt leicht finden und bearbeiten kann.

In der ActiveRoles Server MMC-Schnittstelle können Sie die Berechtigungen für ein Objekt anzeigen, indem Sie einfach auf das Objekt klicken. Die Berechtigungseinträge werden dann in einer zentralen Ansicht angezeigt. Dies erleichtert Administratoren das Überprüfen der Berechtigungen für sicherheitsrelevante Objekte und das Identifizieren möglicher Sicherheitsprobleme.

Verwaltung der einheitlichen Sicherheit

ActiveRoles Server-Zugriffsvorlagen können für die Festlegung von Berechtigungen in Active Directory verwendet werden. Die für die Unterstützung der rollenbasierten Gruppierung von Berechtigungen konzipierten Zugriffsvorlagen bieten einen effizienten Mechanismus für die Einstellung und Aufrechterhaltung der Zugriffskontrolle, wodurch die Verwaltung von Berechtigungen in Active Directory vereinfacht und verbessert wird.

Um diese Funktion bereitzustellen, bietet ActiveRoles Server dem Administrator die Möglichkeit, die einheitliche Sicherheit von Active Directory mit ausgewählten, mit Hilfe von Zugriffsvorlagen festgelegten Berechtigungen zu aktualisieren. Diese Option, die als „Weitergabe von Berechtigungen" bezeichnet wird, soll Benutzern und Anwendungen einheitliche Berechtigungen für Active Directory bereitstellen. Im normalen Betrieb von ActiveRoles Server wird diese Option nicht verwendet.

Für ActiveRoles Server-Berechtigungseinträge, für die die Option der Berechtigungsverbreitung aktiviert ist, generiert ActiveRoles Server Active Directory-native Berechtigungseinträge in Übereinstimmung mit den ActiveRoles Server-Berechtigungen. Nach der Konfiguration gewährleistet diese Option, dass jedes Mal, wenn sich ActiveRoles Server-Berechtigungszuweisungen oder Vorlagen ändern, die zugehörigen nativen Berechtigungseinträge entsprechend geändert werden.

ADSI-Provider und Skriptrichtlinie zur Unterstützung der Anpassung

ActiveRoles Server bietet die Möglichkeit, seine sofort einsetzbaren Funktionen mit Hilfe von Skripts und Anwendungen, die mit dem Verwaltungsdienst interagieren, individuell anzupassen. ActiveRoles Server ermöglicht ein hohes Maß an benutzerdefinierten Änderungen, um den speziellen geschäftlichen und unternehmerischen Anforderungen zu entsprechen. Dies verleiht den Kunden eine höhere Flexibilität bei der Verwendung des Produkts und ermöglicht ihnen, Lösungen zu entwickeln, die ganz einfach in vorhandene Systeme und Daten integriert werden können. Die folgende Liste zeigt einige der Möglichkeiten, wie das Produkt angepasst werden kann:

- Mit Hilfe des ActiveRoles Server ADSI Providers können die vorhandenen proprietären Anwendungen oder benutzerdefinierten webbasierten Schnittstellen mit ActiveRoles Server kommunizieren, um Verwaltungs- und Bereitstellungsaufgaben an Benutzerkonten und Gruppen durchzuführen.
- Mit Hilfe von Richtlinienskripts können benutzerdefinierte Unternehmensregeln erzwungen werden, um Datenformate und administrative Arbeitsabläufe zu regeln.
- Mit Hilfe von Richtlinienskripts können die in einer HR-Datenbank oder in einem ERP-System gespeicherten Daten in die Verwaltung und Bereitstellung von Benutzern integriert werden.

ActiveRoles Server ermöglicht, dass vom Benutzer entwickelte Skripts und Anwendungen Verzeichnisobjekte mit Hilfe des Verwaltungsdienstes manipulieren (*persistente Objekte*) und die Kontrolle über Objekte übernehmen, die gerade mit ActiveRoles Server erstellt, geändert oder gelöscht werden (*in Bearbeitung befindliche Objekte*).

Durch den programmatischen Zugriff auf persistente und in Bearbeitung befindliche Objekte ist die Anpassung von ActiveRoles Server in den beiden nachfolgend aufgeführten Bereichen ganz leicht:

- Erstellen von benutzerdefinierten Anwendungen und Benutzerschnittstellen
- Erzwingen von administrativen Unternehmensrichtlinien durch Ausführung von benutzerdefinierten Skripts (*Skriptrichtlinien*)

Benutzerdefinierte Anwendungen und Benutzerschnittstellen

Für die Manipulation von Verzeichnisobjekten in ActiveRoles Server kann eine benutzerdefinierte Anwendung oder Benutzerschnittstelle erstellt werden. ActiveRoles Server umfasst den ADSI Provider für die Kommunikation mit dem Verwaltungsdienst über standardmäßige COM-Schnittstellen, die der Microsoft ADSI 2.5 Spezifikation entsprechen.

Benutzerdefinierte Anwendungen sind ausführbare Dateien, die Daten für den Verwaltungsdienst bereitstellen oder Daten vom Verwaltungsdienst abrufen und verarbeiten. So kann zum Beispiel eine Organisation mit einer Humanressourcen-Datenbank eine benutzerdefinierte Anwendung entwickeln und bereitstellen, die persönliche Informationen aus der Datenbank extrahiert und dann an den Verwaltungsdienst weiterleitet, um die Bereitstellung von Benutzerkonten zu erleichtern.

Benutzerdefinierte Benutzerschnittstellen sind normalerweise webbasierte Schnittstellen, die bestimmte Aufgaben an die Benutzer übertragen. Benutzerdefinierte Benutzerschnittstellen können auch verwendet werden, um den Arbeitsablauf von Netzwerkadministratoren und Help Desk-Mitarbeitern zu rationalisieren. So können zum Beispiel webbasierte Seiten erstellt werden, sodass Help Desk-Mitarbeitern nur die Felder angezeigt werden, die mit Benutzereigenschaften in Verbindung stehen, die sie gemäß den Unternehmensstandards anzeigen und ändern können.

Sowohl benutzerdefinierte Anwendungen als auch Benutzerschnittstellen beruhen hinsichtlich des Zugriffs auf die Funktionen von ActiveRoles Server auf dem ActiveRoles Server ADSI Provider.

Benutzerdefinierte Skriptrichtlinien

ActiveRoles Server bietet die Möglichkeit, administrative Richtlinien durch die Ausführung von vom Benutzer entwickelten Skripts zu implementieren. Dies ermöglicht folgende Aktionen:

- **Erleichtern der Bereitstellung von Benutzerkonten** Füllen der Benutzereigenschaften durch Integration einer externen Datenbank und Automatisierung von aus mehreren Schritten bestehenden Bereitstellungsaufgaben.
- **Wahrung der Integrität von Verzeichnisinhalten** Verhindern von Inkonsistenzen zwischen Active Directory-Daten durch Erzwingen von Aktualisierungssequenz- und Datenformatrichtlinien im gesamten Unternehmen.
- **Erzwingen von Business-Regeln** Wahrung des Sicherheitskonzepts und Sammeln von Verwaltungserfahrungen durch die Integration von Business-Regeln in den administrativen Arbeitsablauf.

Nach erfolgreicher Konfiguration werden die benutzerdefinierten, skriptbasierten Richtlinien ohne Interaktion mit dem Benutzer erzwungen. ActiveRoles Server handhabt automatisch die Ausführung der Richtlinienskripts, die bestimmte administrative Vorgänge ergänzen und weitere administrative Vorgänge auslösen. Richtlinienskripts können zum Beispiel für folgende Aktionen verwendet werden:

- Durchführen einer hoch entwickelten Gültigkeitsprüfung für Eingangsdaten
- Synchrone Änderung von Informationen in mehreren Datenquellen wie etwa dem Active Directory-Speicher, dem Microsoft Exchange-Server und den Datenbanken des HR- oder ERP-Systems
- Sicherstellen, dass die delegierten Administratoren einen vorgegebenen administrativen Arbeitsablauf einhalten
- Verknüpfen von mehreren Verwaltungsaufgaben in einer Operatortransaktion

Dynamische Gruppen

ActiveRoles Server unterstützt die Rationalisierung der Pflege von Gruppen, indem es die Gruppenmitgliedschaft dynamisch und mit regelbasierten Mitgliedschaftskriterien definiert. Die dynamische Gruppenmitgliedschaft verhindert die Notwendigkeit zur manuellen Aktualisierung von Mitgliedschaftslisten für Sicherheits- und Verteilergruppen.

ActiveRoles Server bietet die folgenden Funktionen zum Automatisieren der Wartung von Gruppenmitgliedschaftslisten:

- Regelbasierter Mechanismus, der immer dann, wenn die Objektattribute in Active Directory geändert werden, automatisch Objekte zu Gruppen hinzufügt und entfernt
- Flexible Mitgliedschaftskriterien, die sowohl das abfragebasierte als auch das statische Füllen von Gruppen ermöglichen

Die Mitgliedschaftskriterien fallen in die folgenden Kategorien:

- **Explizit einschließen** Gewährleistet, dass die angegebenen Objekte unabhängig von jeglichen an den Objekten vorgenommenen Änderungen in der Mitgliedschaftsliste enthalten sind.
- **Nach Abfrage einschließen** Füllt die Mitgliedschaftsliste mit Objekten, die bestimmte Eigenschaften aufweisen. Wenn ein Objekt erstellt wird oder wenn seine Eigenschaften geändert werden, fügt ActiveRoles Server dieses Objekt der Mitgliedschaftsliste hinzu bzw. entfernt es daraus, abhängig davon, ob die Eigenschaften des Objekts den Suchkriterien entsprechen.
- **Gruppenmitglieder einschließen** Füllt die Mitgliedschaftsliste mit Mitgliedern von bestimmten ausgewählten Gruppen. Wenn ein Objekt zu den gewählten Gruppen hinzugefügt oder daraus entfernt wird, fügt ActiveRoles Server das Objekt automatisch zur Mitgliedschaftsliste hinzu oder entfernt es aus dieser.
- **Explizit ausschließen** Gewährleistet, dass die angegebenen Objekte unabhängig von jeglichen an den Objekten vorgenommenen Änderungen nicht in der Mitgliedschaftsliste enthalten sind.
- **Nach Abfrage ausschließen** Gewährleistet, dass Objekte mit bestimmten Eigenschaften nicht in der Mitgliedschaftsliste enthalten sind. ActiveRoles Server entfernt Objekte automatisch aus der Mitgliedschaftsliste, abhängig davon, ob die Eigenschaften der Objekte den Suchkriterien entsprechen.
- **Gruppenmitglieder ausschließen** Gewährleistet, dass Mitglieder der angegebenen Gruppen nicht in der Mitgliedschaftsliste enthalten sind. Wenn ein Objekt einer der ausgewählten Gruppen hinzugefügt wird, entfernt ActiveRoles Server dieses Objekt automatisch aus der Mitgliedschaftsliste.

Diese Mitgliedschaftskriterien gelten auch für verwaltete Einheiten.

Betrieb in Umgebungen mit mehreren Gesamtstrukturen

Active Directory organisiert Netzwerkelemente in einer hierarchischen Struktur auf der Grundlage des Konzepts der Container, wobei der Container der obersten Ebene als eine Gesamtstruktur bezeichnet wird. Heutzutage bestehen zahlreiche Active Directory-Implementierungen aus mehreren Gesamtstrukturen. Die üblichen Gründe für das Vorhandensein von Implementierungen mehrerer Gesamtstrukturen sind die Isolation der administrativen Verwaltungsstellen, Fragen der Organisationsstruktur (z.B. autonome Unternehmenseinheiten und dezentralisierte IT-Abteilungen), die Unternehmensstrategie oder gesetzliche oder behördliche Anforderungen.

Dieser Abschnitt enthält Informationen über die Funktionsmerkmale und Vorzüge von ActiveRoles Server bei Anwendung auf Umgebungen, in denen mehrere Active Directory-Gesamtstrukturen bereitgestellt wurden.

Mit ActiveRoles Server können Sie eine skalierbare, geschützte und verwaltbare Infrastruktur erstellen, die die Benutzer- und Ressourcenverwaltung in einer aus mehreren Gesamtstrukturen bestehenden Umgebung erleichtert. Nachfolgend sind einige der Vorteile der Bereitstellung von ActiveRoles Server in einer solchen Umgebung aufgeführt:

- Zentralisierte Verwaltung von Verzeichnisdaten in Domänen, die zu verschiedenen Gesamtstrukturen gehören
- Administrative Ansichten, die die Grenzen der Gesamtstruktur überschreiten
- Möglichkeit zum Delegieren der administrativen Kontrolle über Verzeichnisdaten, wo dies angebracht ist, ohne Berücksichtigung der Grenzen der Gesamtstruktur
- Richtlinienbasierte Kontrolle und Automatisierung der Verwaltung der Verzeichnisdaten über die Grenzen von Gesamtstrukturen hinweg

Durch die Registrierung von Active Directory-Domänen bei ActiveRoles Server bilden Sie eine Zusammenstellung verwalteter Domänen, die eine ActiveRoles Server-Sicherheits- und Verwaltungsgrenze in Active Directory darstellt. Die Zusammenstellung muss nicht auf Domänen aus einer einzigen Gesamtstruktur beschränkt sein. Sie können Domänen aus jeder Gesamtstruktur in Ihrer Umgebung registrieren und den ActiveRoles Server Verwaltungsdienst so konfigurieren, dass er die entsprechenden administrativen Rechtezuweisungen auf Domänenbasis verwendet.

Um die Verwaltung von Verzeichnisdaten innerhalb der verwalteten Domänen zu zentralisieren, fragt ActiveRoles Server die Active Directory Schemadefinitionen von allen Gesamtstrukturen, zu denen diese Domänen gehören, ab und konsolidiert sie. Die konsolidierte Schemabeschreibung wird in der ActiveRoles Server Konfigurationsdatenbank gespeichert und enthält Informationen über die Objektklassen und die Attribute der Objektklassen, die in den verwalteten Domänen gespeichert werden können. Durch die Verwendung des konsolidierten Schemas erweitert ActiveRoles Server den Umfang seiner administrativen Vorgänge, um so die gesamte Zusammenstellung der verwalteten Domänen unabhängig von den Grenzen der Gesamtstruktur abzudecken.

ActiveRoles Server ermöglicht Administratoren, Verzeichnisobjekte (wie etwa Benutzer, Gruppen, Computer usw.) in einer relationalen Struktur zu organisieren, die aus regelbasierten administrativen Ansichten (bezeichnet als „verwaltete Einheiten“) besteht und von denen jede nur die Objekte umfasst, die bestimmmte, vom Administrator definierte Mitgliedschaftskriterien erfüllen. Diese Struktur kann unabhängig von logischen Modell von Active Directory erstellt werden, das auf dem Konzept der Container beruht und somit starre Grenzen zwischen Containern impliziert, ganz gleich, ob es sich dabei

um Gesamtstrukturen, Domänen oder Organisationseinheiten handelt. Administratoren können verwaltete Einheiten so konfigurieren, dass jede Einheit die entsprechende Zusammenstellung von Verzeichnisobjekten repräsentiert, die im selben Active Directory-Container oder in verschiedenen Containern vorhanden sind, wobei verschiedene Gesamtstrukturen nicht die Ausnahme sind.

Um die Verwaltung von Verzeichnisdaten zu erleichtern, bietet ActiveRoles Server eine administrative Delegation auf der Ebene der verwalteten Einheit sowie auf der Ebene der einzelnen Container in Active Directory. Durch die Delegation kann die Autorität über Verzeichnisobjekte, die sich in einer bestimmten Einheit oder in einem bestimmten Container befinden, an gewisse Benutzer oder Gruppen übertragen werden. Die Delegation der Kontrolle über verwaltete Einheiten bietet die Möglichkeit, die Verwaltung von Verzeichnisdaten auf Einzelpersonen aufzuteilen, denen zugetraut wird, die Verwaltung von bestimmten Gruppen und Objekttypen durchzuführen, ohne die Position der Objekte in der Active Directory-Struktur zu berücksichtigen. Folglich erleichtert ActiveRoles Server die Delegation der Kontrolle über Verzeichnisdaten aus einer Gesamtstruktur an Benutzer oder Gruppen, die sich in derselben oder in einer anderen Gesamtstruktur befinden.

ActiveRoles Server bietet außerdem eine regelbasierte Kontrolle und Automatisierung der Verwaltung von Verzeichnisdaten, die auf der Ebene der verwalteten Einheit implementiert werden soll. Durch die Anwendung von Richtlinien und Automatisierungsregeln auf verwaltete Einheiten können Administratoren eine konsistente Kontrolle einer genau definierten Zusammenstellung von Verzeichnisobjekten, die sich in verschiedenen Organisationseinheiten, Domänen oder Gesamtstrukturen befinden, gewährleisten. Darüber hinaus können Richtlinien und Automatisierungsregeln einheitlich auf verschiedene Container – ob in derselben Gesamtstruktur oder in verschiedenen Gesamtstrukturen – angewandt werden, was eine Plattform für komplexe Automatisierungsszenarien bietet, die auch gesamtstrukturübergreifende Vorgänge umfassen können. Ein Beispiel ist die Bereitstellung von Ressourcen einer Gesamtstruktur für die Benutzer einer anderen Gesamtstruktur.

Beim Hinzufügen von Objekten zu einer Gruppe ermöglicht ActiveRoles Server die Auswahl von Objekten aus verschiedenen verwalteten Domänen einschließlich derer, die zu unterschiedlichen Gesamtstrukturen gehören. Dieser Vorgang erfordert eine Vertrauensstellung zwischen der Domäne, in der sich die Gruppe befindet, und der Domäne, in der sich das Objekt befindet, das Sie zur Gruppe hinzufügen möchten. Ansonsten weist Active Directory den Vorgang zurück und daher ermöglicht Ihnen ActiveRoles Server nicht die Auswahl des Objekts. Beachten Sie, dass Active Directory automatisch Vertrauensstellungen zwischen Domänen innerhalb einer Gesamtstruktur erstellt. Für Domänen in unterschiedlichen Gesamtstrukturen müssen Administratoren explizit Vertrauensstellungen definieren.

Die regelbasierten Mechanismen, die ActiveRoles Server für das automatische Füllen von Gruppen bietet, können auch in aus mehreren Gesamtstrukturen bestehenden Umgebungen frei gewählt werden. Sie können Regeln so konfigurieren, dass ActiveRoles Server Gruppen mit Objekten füllt, die sich in verschiedenen Domänen befindet. Dabei ist es unerheblich, ob sich diese in ein und derselben Gesamtstruktur oder in verschiedenen Gesamtstrukturen befinden. Die Fähigkeiten zur automatischen Verwaltung von Gruppenmitgliedschaftslisten von ActiveRoles Server sind auch durch die Active Directory-Bedingungen beschränkt, die besagen, dass eine Gruppe nur Objekte aus der Domäne, in der sich die Gruppe befindet, oder aus den Domänen, die eine Vertrauensstellung zu dieser Domäne haben, beinhalten kann. Mit anderen Worten, wenn keine Vertrauensstellung zwischen der Domäne, in der sich die Gruppe befindet, und der Domäne, die ein bestimmtes Objekt enthält, besteht, kann das Objekt weder manuell noch automatisch durch ActiveRoles Server zur Gruppe hinzugefügt werden.

Unterstützung des Exchange-Ressourcen-Gesamtstrukturmodells

Mit der Bereitstellung von mehreren Gesamtstrukturen entsteht der Bedarf nach gesamtstruktur-übergreifenden Kollaborationslösungen. Die wichtigste dieser Lösungen ist das auf Exchange Server basierende Nachrichtenübertragungssystem. Bei mehreren Gesamtstrukturen ist eine der Optionen für die Integration von Exchange in Active Directory das Ressourcen-Gesamtstrukturmodell. ActiveRoles Server bietet eine Lösung, die die Verwaltung von Exchange-Postfächern in aus mehreren Gesamt-strukturen bestehenden Umgebungen, die das Exchange-Ressourcen-Gesamtstrukturmodell nutzen, erleichtert.

Das Exchange-Ressourcen-Gesamtstrukturmodell beinhaltet eine separate Active Directory-Gesamtstruktur, die der Ausführung von Exchange und dem Hosten von Postfächern dient. Benutzerkonten befinden sich in einer oder mehreren Konto-Gesamtstrukturen, die von der Exchange-Ressourcen-Gesamtstruktur getrennt sind. Da eine Exchange-Organisation die Grenzen einer Gesamtstruktur nicht überschreiten kann, erfordert die Bereitstellung eines Postfachs für ein Benutzerkonto die Erstellung eines separaten, Postfach-fähigen Kontos in der Exchange-Ressourcen-Gesamtstruktur und die Verknüpfung mit diesem Benutzerkonto.

Um also über eine Exchange-Ressourcen-Gesamtstruktur zu verfügen, die von den Konto-Gesamt-strukturen getrennt ist, ist eine Verzeichnissynchronisation zwischen der Ressourcen-Gesamtstruktur und den Konto-Gesamtstrukturen erforderlich. Es muss ein Bereitstellungsprozess konfiguriert werden, sodass jedes Mal, wenn der Administrator ein Benutzerkonto in einer Konto-Gesamtstruktur erstellt, ein Postfach-fähiges Konto in der Exchange-Ressourcen-Gesamtstruktur erstellt wird. Die Konto-eigenschaften müssen auch zwischen der Konto-Gesamtstruktur und der Ressourcen-Gesamtstruktur synchronisiert werden. ActiveRoles Server automatisiert diese Prozesse durch die Implementierung einer Lösung, die die folgenden Funktionen umfasst:

- **Automatische Postfachbereitstellung** Erstellt automatisch Postfach-fähige Konten in der Ressourcen-Gesamtstruktur und verknüpft sie mit Benutzerkonten in Konto-Gesamtstrukturen.
- **Synchronisation** Aktualisiert automatisch Verzeichnisdaten in der Ressourcen-Gesamt-struktur, um die Aktualisierungen an Benutzerkonten in Konto-Gesamtstrukturen widerzu-spiegeln.
- **Postfachdeprovisionierung** Entfernt den Zugriff auf Benutzerpostfächer in der Ressourcen-Gesamtstruktur bei Deaktivierung (Deprovisionierung) von Benutzerkonten in Konto-Gesamtstrukturen.
- **Postfachlöschung** Löscht Postfach-fähige Konten in der Ressourcen-Gesamtstruktur beim Löschen von Benutzerkonten in Konto-Gesamtstrukturen.

Mit diesen Funktionen bietet ActiveRoles Server eine administrative Lösung, die den gesamten Lebenszyklus von Benutzerpostfächern in einer Active Directory-Umgebung, die das Exchange-Ressourcen-Gesamtstrukturmodell nutzt, abdeckt.

2

Erste Schritte

- Starten der ActiveRoles Server-Konsole
- Überblick über die Benutzerschnittstelle
- Ansichtsmodus
- Verwenden verwalteter Einheiten
- Einrichten eines Filters
- Suchen nach Objekten
- Abrufen richtlinienbezogener Informationen

Starten der ActiveRoles Server-Konsole

Die ActiveRoles Server-Konsole, auch als MMC-Benutzeroberfläche bezeichnet, ist ein umfassendes Verwaltungstool für Active Directory und Microsoft Exchange. Die ActiveRoles Server-Konsole erleichtert die Suche nach Verzeichnisobjekten und die Ausführung von Verwaltungsaufgaben.

Gehen Sie folgendermaßen vor, um die ActiveRoles Server-Konsole zu starten:

- Zeigen Sie auf **Starten | Programme | Quest Software | ActiveRoles Server** und klicken Sie dann auf **ActiveRoles Server-Konsole**.

Normalerweise wählt die ActiveRoles Server-Konsole automatisch den Verwaltungsdienst aus und stellt eine Verbindung her. Wenn die Konsole keine Verbindung zum Verwaltungsdienst herstellen kann oder Sie den Verwaltungsdienst manuell auswählen möchten, finden Sie im Abschnitt „Verbinden mit dem Verwaltungsdienst" im ActiveRoles Server-Administratorhandbuch weitere Informationen.

Aufrufen und Verwenden der Hilfe

ActiveRoles Server-Hilfe erläutert die Konzepte und umfasst Anweisungen für die Durchführung von Aufgaben mit dem Produkt.

Gehen Sie wie nachfolgend beschrieben vor, um während Ihrer Arbeit die Hilfe aufzurufen:

- Um die ActiveRoles Server-Hilfe aufzurufen, klicken Sie auf **Hilfe** im Menü **Aktion** oder auf **Hilfethemen** im Menü **Hilfe**.
- Um die Beschreibung eines Dialogfelds anzuzeigen, klicken Sie auf die Schaltfläche **Hilfe** im Dialogfeld oder drücken Sie die Taste F1.
- Um eine Kurzbeschreibung eines Menübefehls oder einer Schaltfläche auf einer Symbolleiste anzuzeigen, zeigen Sie mit der Maus auf den Befehl oder die Schaltfläche. Die Beschreibung wird in der Statusleiste unten im Fenster angezeigt.

Dieses Handbuch verweist auf Hilfethemen, indem es Pfade zu den Themen in der Struktur angibt, die auf der Registerkarte **Inhalt** im Hilfefenster angezeigt werden. Um beispielsweise auf das Thema zuzugreifen, auf das mit **Anleitungen/Suchen nach Objekten** verwiesen wird, erweitern Sie nacheinander die Überschriften **Quest ActiveRoles Server** und **Anleitungen** und klicken dann unter **Anleitungen** auf **Suchen nach Objekten**.

Sie können ein einzelnes Hilfethema oder alle Hilfethemen unter einer ausgewählten Überschrift drucken.

Gehen Sie folgendermaßen vor, um ein einzelnes Hilfethema zu drucken:

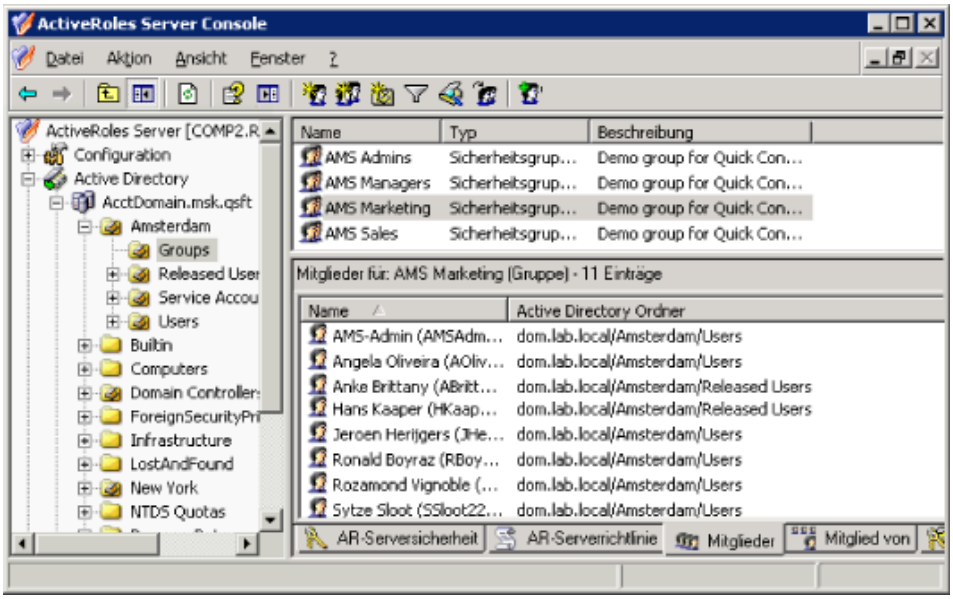
1. Klicken Sie in der Menüleiste auf **Hilfe** und klicken Sie dann auf **Hilfethemen**.
2. Erweitern Sie im linken Bereich des Hilfe-Viewers die Überschrift, die das zu druckende Thema enthält, und klicken Sie dann auf das Thema.
3. Klicken Sie in der Symbolleiste des Hilfefensters auf **Optionen** und klicken Sie dann auf **Drucken**.
4. Klicken Sie auf **OK**, um nur das ausgewählte Thema zu drucken.

Gehen Sie folgendermaßen vor, um alle Hilfethemen unter einer Überschrift zu drucken:

1. Klicken Sie in der Menüleiste auf **Hilfe** und klicken Sie dann auf **Hilfethemen**.
2. Klicken Sie im linken Bereich des Hilfefensters auf die Überschrift, die die Themen enthält, die Sie drucken möchten.
3. Klicken Sie in der Symbolleiste des Hilfefensters auf **Optionen** und klicken Sie dann auf **Drucken**.
4. Klicken Sie im Dialogfeld **Themen drucken** auf **Ausgewählte Überschrift und alle Unterthemen drucken** und klicken Sie dann auf **OK**.

Überblick über die Benutzerschnittstelle

Nach dem Start der ActiveRoles Server-Konsole wird ein Fenster angezeigt, das dem folgenden ähnelt.



Der linke Fensterbereich enthält die Konsolenstruktur, in der die im Snap-In verfügbaren Elemente angezeigt werden. Der rechte Fensterbereich, der auch Detailfenster genannt wird, zeigt Informationen zu den in der Konsolenstruktur ausgewählten Elementen an. Sie können in diesem Bereich die meisten Verwaltungsaufgaben ausführen, indem Sie Befehle im Menü **Aktion** verwenden.

Weitere Informationen werden im unteren Teilbereich des Bereichs „Details" angezeigt, wenn Sie die Option **Erweiterte Detailansicht** im Menü **Ansicht** aktivieren. Ausgehend von diesem Teilbereich können Sie Verwaltungsaufgaben mit Hilfe der Befehle im Menü **Aktion** durchführen.

Konsolenstruktur

Der linke Bereich der ActiveRoles Server-Konsole enthält die Konsolenstruktur.

Das Stammverzeichnis der Konsolenstruktur wird als **ActiveRoles Server** bezeichnet. Der Name des Verwaltungsdienstes wird in eckigen Klammern angezeigt. Wenn Sie für die Anzeige der ActiveRoles Server-Konsole die erweiterte Ansicht ausgewählt haben (**Ansicht | Modus**), werden die folgenden Ordner unter dem Stammverzeichnis der Konsolenstruktur angezeigt:

- **Configuration** Enthält alle systemeigenen Objekte von ActiveRoles Server in Containern mit entsprechenden Namen.
- **Active Directory** Enthält eine Liste der bei ActiveRoles Server registrierten Domänen. In diesem Ordner können Sie Domänen durchsuchen, um Verzeichnisobjekte (Benutzer, Gruppen, Computer) anzuzeigen, sowie Verwaltungsaufgaben für diese Objekte ausführen.
- **AD LDS (ADAM)** Enthält eine Liste der bei ActiveRoles Server registrierten AD LDS-Verzeichnispartitionen. In diesem Ordner können Sie die Partitionen nach Verzeichnisobjekten (Benutzern, Gruppen, Containern) durchsuchen und Verwaltungsaufgaben an diesen Objekte durchführen.
- **Applications** Enthält eine Liste der in ActiveRoles Server integrierten Anwendungen wie etwa das Berichtswesen und ermöglicht einen schnellen Zugriff auf diese Anwendungen.

Der Ansichtsmodus für die Konsole bestimmt, welche Ordner in der Konsolenstruktur angezeigt werden. Ausführlichere Informationen finden Sie unter „Ansichtsmodus" weiter unten in diesem Dokument.

Bereich „Details"

Wenn Sie ein Element in der Konsolenstruktur auswählen, ändert sich die Anzeige im Bereich „Details" entsprechend. Um Verwaltungsaufgaben auszuführen, klicken Sie auf die Elemente im Bereich „Details" und verwenden Sie die Befehle im Menü **Aktion**. Die **Aktion**-Menübefehle werden auch im Kontextmenü angezeigt, das Sie aufrufen, indem Sie mit der rechten Maustaste auf Elemente in der Konsolenstruktur oder im Bereich „Details" klicken.

Standardmäßig sind die im Bereich „Details" aufgeführten Objekte in aufsteigender Reihenfolge nach ihrem Objektnamen sortiert. Sie können die Sortierreihenfolge ändern, indem Sie auf eine Spaltenüberschrift klicken. Mit dem Befehl **Spalten auswählen** im Menü **Ansicht** können Sie Spalten zum Bereich „Details" hinzufügen bzw. aus ihm entfernen.

In der ActiveRoles Server-Konsole können Sie Filter auf den Bereich „Details" anwenden, um nach Verzeichnisobjekten zu suchen. Um einen Filter zu konfigurieren, wählen Sie eine Domäne aus und klicken Sie dann auf **Filteroptionen** im Menü **Ansicht**. Es ist auch möglich, ein Objekt im Bereich „Details" zu suchen, indem Sie einige Zeichen eingeben. Hierdurch wird das erste Element in der sortierten Spalte markiert, das mit den von Ihnen eingegebenen Zeichen übereinstimmt.

Bereich „Erweitert"

Der Bereich „Erweitert" wird unten im Bereich „Details" angezeigt, wenn Sie die Option **Erweiterte Detailansicht** im Menü **Ansicht** aktivieren. Sie können den Bereich „Erweitert" verwenden, um ein in der Konsolenstruktur oder im Bereich „Details" ausgewähltes Objekt zu verwalten: Klicken Sie mit der rechten Maustaste auf einen in der Liste vorhandenen Eintrag, um diesen zu verwalten, oder klicken Sie mit der rechten Maustaste auf einen leeren Bereich des Bereichs „Erweitert", um einen neuen Eintrag hinzuzufügen.

Der Bereich „Erweitert" besteht aus einer Reihe von Seiten mit verschiedenen Registerkarten. Das ausgewählte Objekt legt fest, welche Registerkarten angezeigt werden. Nachfolgend sind alle Registerkarten einschließlich einer Beschreibung aufgeführt, die im Bereich „Erweitert" angezeigt werden können:

- **AR-Serversicherheit** Listet die auf das ausgewählte Objekt angewandten ActiveRoles Server-Zugriffsvorlagen auf.
- **Verknüpfungen** Listet die Objekte auf, auf die die ausgewählte Zugriffsvorlage angewendet wird.
- **AR-Serverrichtlinie** Listet die Richtlinienobjekte von ActiveRoles Server auf, die auf das ausgewählte Objekt angewendet werden.
- **Einheitliche Sicherheit** Listet die für das ausgewählte Objekt festgelegten Active Directory-Berechtigungseinträge auf.
- **Mitglied von** Listet die Gruppen auf, zu denen das ausgewählte Objekt gehört.
- **Mitglieder** Listet die Mitglieder der ausgewählten Gruppe auf.

Die ActiveRoles Server-Konsole zeigt die Registerkarten **AR-Serversicherheit**, **AR Serverrichtlinie** und **Einheitliche Sicherheit** für ein ausgewähltes Objekt nur dann an, wenn Ihr Benutzerkonto über die Berechtigung **Lesekontrolle** für das ausgewählte Objekt verfügt.

Abhängig von der von Ihnen im Bereich „Erweitert" ausgewählten Registerkarte zeigt die Symbolleiste die folgenden Schaltflächen an, um Sie bei der Arbeit mit den Einträgen auf der Registerkarte zu unterstützen:

AR-Serversicherheit, Verknüpfungen

	Wenden Sie weitere Zugriffsvorlagen auf das ausgewählte Objekt an.
	Zeigen Sie Zugriffsvorlagen an, die aufgrund von Vererbung Auswirkungen auf das ausgewählte Objekt haben.
	Synchronisieren Sie von ActiveRoles Server-Sicherheit zu Active Directory-Sicherheit.

AR-Serverrichtlinie

	Wenden Sie weitere Richtlinienobjekte auf das ausgewählte Objekt an.
	Zeigen Sie Richtlinienobjekte an, die aufgrund von Vererbung Auswirkungen auf das ausgewählte Objekt haben.

Einheitliche Sicherheit

	Zeigen Sie Berechtigungseinträge an, die von übergeordneten Objekten geerbt werden.
	Zeigen Sie Standard-Berechtigungseinträge an, die vom AD-Schema angegeben werden.

Mitglied von, Mitglieder

	Fügen Sie das ausgewählte Objekt zu Gruppen hinzu.
	Legen Sie die Gruppe als primäre Gruppe für das ausgewählte Objekt fest.

Ansichtsmodus

In der ActiveRoles Server-Konsole können Sie den Ansichtsmodus wählen – Standard, Erweitert oder Roh. Die Änderung des Ansichtsmodus ermöglicht Ihnen, erweiterte Objekte und Container aus der Anzeige herauszufiltern.

Im Standardmodus werden Active Directory-Objekte und verwaltete Einheiten angezeigt. Objekte und Container, die mit der ActiveRoles Server-Konfiguration in Zusammenhang stehen, werden herausgefiltert. Der Standardmodus sollte normalerweise von delegierten Administratoren und Help Desk-Mitarbeitern verwendet werden.

Der erweiterte Modus zeigt alle Objekte und Container mit Ausnahme der für interne Verwendungszwecke von ActiveRoles Server reservierten Objekte und Container an. Der erweiterte Modus ist für Administratoren konzipiert, die für die Konfiguration des Systems und für die Verwaltung von proprietären ActiveRoles Server-Objekten verantwortlich sind.

Im Rohmodus werden alle Objekte und Container angezeigt, die im Namespace von ActiveRoles Server definiert sind. Dieser Modus wurde primär für die Problembehandlung entworfen.

Im Rohmodus zeigt die Konsole alle Daten an, die sie vom Verwaltungsdienst empfängt. Im Standard- oder erweiterten Modus werden einige Daten herausgefiltert. So wird im Standardmodus beispielsweise nicht der Ordner **Konfiguration** in der Konsolenstruktur angezeigt. Ein anderes Beispiel ist der Ordner **Konfigurationscontainer**, in dem der Namenskontext der Active Directory-Konfiguration angezeigt wird. Dieser Ordner wird nur im Rohmodus angezeigt. Auch einige Befehle und Eigenschaftenseiten werden nur im Rohmodus der Konsole angezeigt.

Im Rohmodus wird im Snap-In also alles angezeigt, was angezeigt werden kann. Andernfalls werden einige Elemente ausgeblendet. Beachten Sie, dass durch die Änderung des Ansichtsmodus kein Element geändert wird. Es werden lediglich bestimmte Elemente am Bildschirm angezeigt oder ausgeblendet.

Um den Ansichtsmodus zu ändern, klicken Sie auf **Modus** im Menü **Ansicht**. Klicken Sie im Dialogfeld **Ansichtsmodus** auf **Standardmodus**, **Erweiterter Modus** oder **Rohmodus**.

Kontrollierte Objekte

Die ActiveRoles Server-Konsole bietet einen visuellen Hinweis auf Objekte, auf die die Zugriffsvorlage, Richtlinienobjekte oder Gruppenrichtlinienobjekte angewandt werden. Diese Objekte werden durch einen grünen Pfeil auf dem normalen Objektsymbol markiert: .

Um Objekte zu markieren, klicken Sie im Menü **Ansicht** auf **Kontrollierte Objekte markieren**. Aktivieren Sie die Kontrollkästchen, um die zu markierenden Objektkategorien anzugeben, und klicken Sie dann auf **OK**.

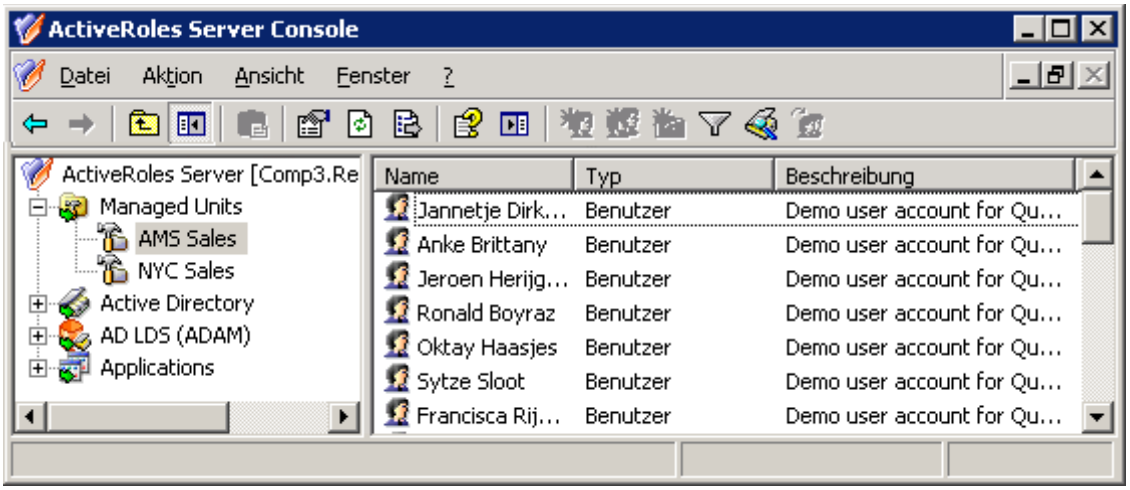
Verwenden verwalteter Einheiten

ActiveRoles Server umfasst die folgenden grundlegenden Sicherheits- und Verwaltungselemente:

- **Trustees** Benutzer oder Gruppen, die über die Berechtigungen zur Verwaltung von Benutzern, Gruppen, Computern oder anderen Verzeichnisobjekten verfügen.
- **Berechtigungen und Rollen** Berechtigungen sind in Zugriffsvorlagen (Rollen) gruppiert, die definieren, wie ein Trustee Verzeichnisobjekte verwalten kann.
- **Verwaltete Einheiten** Auflistungen von Verzeichnisobjekten, die für die Verwaltung an Trustees delegiert werden.

Der Verzeichnisadministrator legt fest, welche Benutzer oder Gruppen Trustees sind, welche Rollen und Berechtigungen den Trustees zugewiesen sind und welche Objekte in den verwalteten Einheiten enthalten sind.

Mit verwalteten Einheiten wird bestimmt, welche Verzeichnisobjekte ein Trustee verwalten kann. Als Trustee können Sie die verwalteten Einheiten administrieren, für die Ihnen Berechtigungen zugewiesen sind. Verwaltete Einheiten, die Objekte enthalten, die Sie verwalten dürfen, werden in der Konsolenstruktur unter **Managed Units** angezeigt. Die Standardansicht zeigt verwaltete Einheiten und deren Mitglieder wie in der folgenden Abbildung gezeigt an.



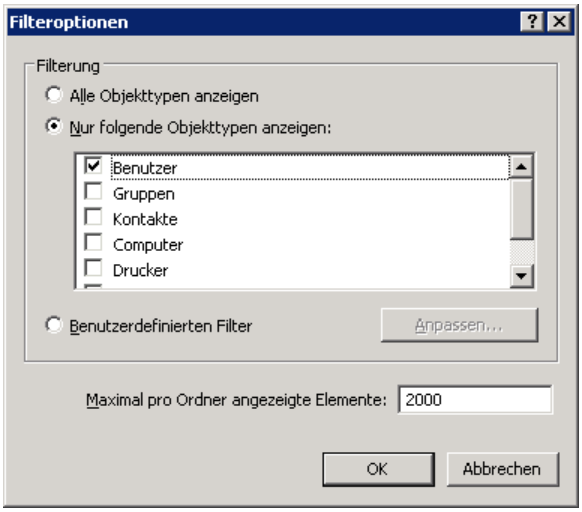
Wenn Sie eine verwaltete Einheit in der Konsolenstruktur auswählen, zeigt der Bereich „Details" eine Liste der in dieser verwalteten Einheit enthaltenen Objekte an. Um Objekte zu verwalten, wählen Sie sie in der Liste aus und verwenden Sie die Befehle im Menü **Aktion**.

Wenn eine verwaltete Einheit einen Container wie etwa eine Organisationseinheit enthält, dann wird der Container in der Konsolenstruktur unter „Verwaltete Einheit" wie in der Abbildung dargestellt angezeigt. Wenn Sie einen Container in der Konsolenstruktur auswählen, werden im Bereich „Details" alle in diesem Container enthaltenen untergeordneten Objekte und Subcontainer aufgelistet.

Einrichten eines Filters

Die ActiveRoles Server-Konsole ermöglicht die Anwendung eines Filters, um nur die Objekte anzuzeigen, die den Filterkriterien entsprechen. Um einen Filter anzuwenden, wählen Sie ein Active Director-Objekt oder einen Container aus und klicken Sie dann auf die Schaltfläche **Filter** in der Symbolleiste: .

Hierdurch wird das Dialogfeld **Filteroptionen** angezeigt, das dem in der folgenden Abbildung dargestellten Dialogfeld entspricht.



Nachdem Sie den Filter festgelegt haben, werden die Filterkriterien sofort auf alle Active Directory-Objektlisten in der ActiveRoles Server-Konsole angewandt.

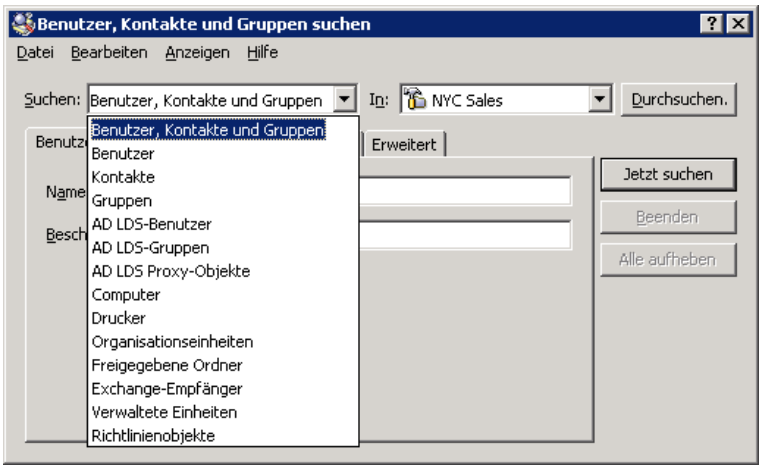
Anweisungen bezüglich der Festlegung von Filteroptionen finden Sie unter **Anleitungen/Ändern von Ansichten/Sortieren und Filtern von Listen in der Detailanzeige** in der ActiveRoles Server-Hilfe.

Suchen nach Objekten

In der ActiveRoles Server-Konsole können Sie mit Hilfe des Fensters **Suchen** nach Objekten verschiedenen Typs suchen. Um das Fenster **Suchen** aufzurufen, klicken Sie mit der rechten Maustaste auf einen Container und klicken dann auf **Suchen**.

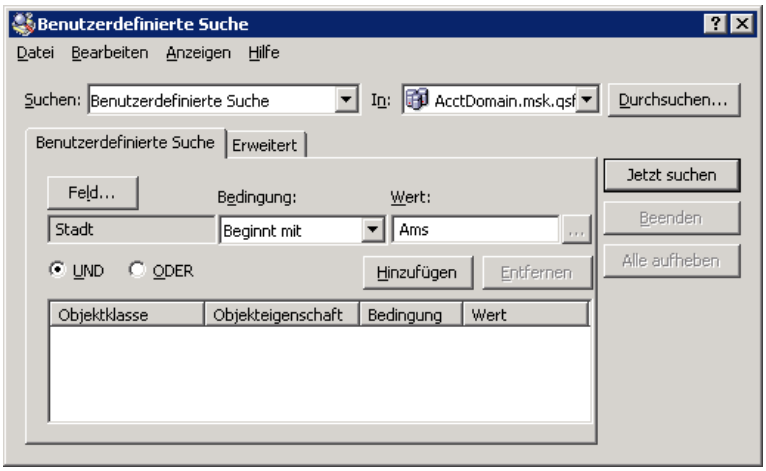
In der Liste **In** können Sie den zu suchenden Container oder die zu suchende verwaltete Einheit auswählen. Die Liste enthält den Container, den Sie vor dem Aufruf des Fensters **Suchen** ausgewählt haben. Klicken Sie auf **Durchsuchen**, um Container zur Liste hinzuzufügen.

In der Liste **Suchen** können Sie den Objekttyp auswählen, den Sie suchen möchten (siehe folgende Abbildung).



Wenn Sie einen Objekttyp auswählen, wird das Fenster **Suchen** entsprechend geändert. Beispielsweise wird mit **Benutzer, Kontakte und Gruppen** nach Benutzern, Kontakten oder Gruppen gesucht, indem Kriterien wie der Benutzername, eine beschreibende Notiz zu einem Kontakt oder der Name einer Gruppe verwendet werden. In der Liste **Suchen** teilt ActiveRoles Server die Kategorie **Benutzer, Kontakte und Gruppen** auf, um so eine rationalisierte Suche zu ermöglichen.

Durch Auswahl von **Benutzerdefinierte Suche** aus der Liste **Suchen** können Sie benutzerdefinierte Suchanfragen mit Hilfe der erweiterten Suchoptionen erstellen:



Im Fenster **Suchen** können Sie nach beliebigen Verzeichnisobjekten suchen, z.B. nach Benutzern, Gruppen, Computern, Organisationseinheiten, Druckern oder freigegebenen Ordnern. Sie können auch nach Konfigurationsobjekten von ActiveRoles Server suchen, z.B. nach Zugriffsvorlagen, verwalteten Einheiten und Richtlinienobjekten. Wenn Sie nach Zugriffsvorlagen, Richtlinienobjekten oder verwalteten Einheiten suchen und in der Liste **Suchen** einen entsprechenden Objekttyp auswählen, wird der jeweilige Container in der Liste **In** angezeigt.

Wenn die Suche abgeschlossen ist, werden die den Suchkriterien entsprechenden Objekte (die Suchergebnisse) unten im Fenster **Suchen** aufgelistet. Sie können auf schnelle Art ein Objekt in der Suchergebnisliste finden, indem Sie einige Zeichen eingeben. Hierdurch wird der erste Name ausgewählt, der mit den von Ihnen eingegebenen Zeichen übereinstimmt.

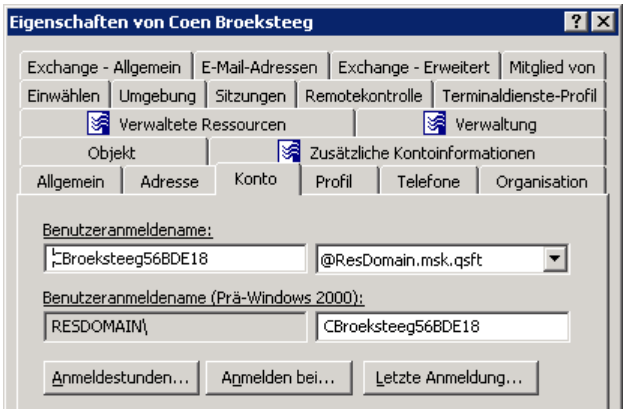
Wenn Sie das Objekt gefunden haben, können Sie es verwalten, indem Sie den Eintrag in der Suchergebnisliste mit der rechten Maustaste anklicken und dann auf die Befehle im Kontextmenü klicken.

Schrittweise Anleitungen bezüglich der Durchführung einer Suche finden Sie unter **Anleitungen/Suche nach Objekten** in der ActiveRoles Server-Hilfe.

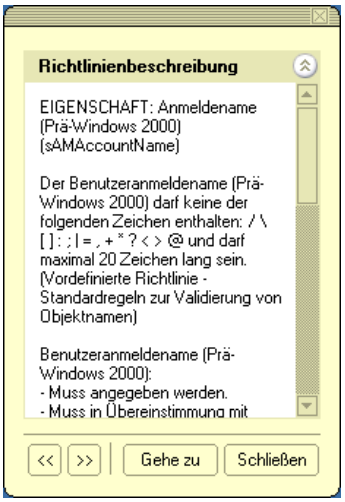
Abrufen richtlinienbezogener Informationen

In Assistenten zur Objekterstellung und in Eigenschafts-Dialogfeldern können einige Eigenschaftsnamen als Hyperlinks angezeigt werden. Dies zeigt an, dass ActiveRoles Server Richtlinieneinschränkungen für die Eigenschaft durchsetzt.

In der folgenden Abbildung sind die Beschriftungen **Benutzeranmeldename** und **Benutzeranmeldename (Prä-Windows 2000)** unterstrichen. Dies bedeutet, dass diese Eigenschaften von einer bestimmten Richtlinie gesteuert werden, die mit ActiveRoles Server definiert wurde.



Um die Richtlinie eingehend zu überprüfen, können Sie auf deren Bezeichnung klicken. Wenn Sie beispielsweise auf **Benutzeranmeldename (Prä-Windows 2000)** klicken, zeigt die ActiveRoles Server-Konsole ein Fenster an, dass dem in der folgenden Abbildung dargestellten Fenster entspricht.

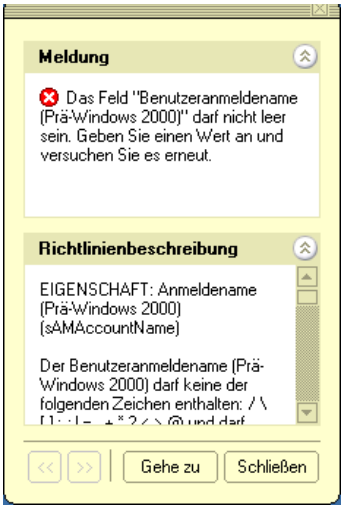

Richtlinienbeschreibung
EIGENSCHAFT: Anmeldename (Prä-Windows 2000) (sAMAccountName)
Der Benutzeranmeldename (Prä-Windows 2000) darf keine der folgenden Zeichen enthalten: / \ [ ] : ; | = , + * ? < > @ und darf maximal 20 Zeichen lang sein. (Vordefinierte Richtlinie - Standardregeln zur Validierung von Objektnamen)
Benutzeranmeldename (Prä-Windows 2000):
- Muss angegeben werden.
- Muss in Übereinstimmung mit
<<
>>
Gehe zu
Schließen

Im Fenster können die folgenden Informationen angezeigt werden:

- **Richtlinienbeschreibung** Bietet eine Kurzbeschreibung der Richtlinie.
- **Meldung** Zeigt Details bezüglich des Problems an, wenn der angegebene Eigenschaftswert gegen die Richtlinie verstößt.

Sie können auf die Pfeile in der oberen linken Ecke klicken, um die Beschreibung anderer, für die angegebene Eigenschaft geltender Richtlinien anzuzeigen.

Der Abschnitt **Meldung** wird immer dann angezeigt, wenn der angegebene Eigenschaftswert gegen die Richtlinie verstößt. Die folgende Abbildung zeigt eine Situation, in der kein Wert für eine obligatorische Eigenschaft angegeben wurde.


Meldung
Das Feld "Benutzeranmeldename (Prä-Windows 2000)" darf nicht leer sein. Geben Sie einen Wert an und versuchen Sie es erneut.
Richtlinienbeschreibung
EIGENSCHAFT: Anmeldename (Prä-Windows 2000) (sAMAccountName)
Der Benutzeranmeldename (Prä-Windows 2000) darf keine der folgenden Zeichen enthalten: / \
<<
>>
Gehe zu
Schließen

Wenn Sie in diesem Fenster auf **Gehe zu** klicken, verschiebt die Konsole den Mauszeiger auf das Feld, das korrigiert werden muss. Sie können einen geeigneten Wert eingeben oder auswählen, um Ihre Eingabe zu korrigieren.

3

Regelbasierte administrative Ansichten

- Verwaltete Einheiten
- Administration verwalteter Einheiten
- Szenario: Implementieren der rollenbasierten Verwaltung über mehrere Organisationseinheiten hinweg

Verwaltete Einheiten

Unternehmen entwerfen ihre auf Organisationseinheiten basierende Netzwerkstruktur meist anhand geografischer Grenzen oder Abteilungsgrenzen. Dies schränkt ihre Möglichkeiten ein, die Verwaltung außerhalb dieser Grenzen zu delegieren. Es können jedoch Situationen entstehen, in denen Objekten anders gruppiert werden müssen, als die auf Organisationseinheiten basierende Struktur vorsieht.

Active Directory bietet ein umfassendes Delegierungsmodell. Da der Delegierungsbereich jedoch anhand von Organisationseinheiten definiert ist, ist die verteilte Verwaltung in Active Directory entsprechend eingeschränkt.

In Active Directory ist es ohne Änderungen der Verzeichnisstruktur nicht möglich, Objekte so neu zu gruppieren, dass die neuen „Gruppen" die Vererbung für ihre Mitglieder beim Delegieren der Kontrolle oder Durchsetzen von Richtlinien unterstützen. Als Lösung für diese unflexible, auf Organisationseinheiten basierende Struktur ermöglicht ActiveRoles Server das Konfigurieren administrativer Ansichten, die alle Anforderungen an die Verzeichnisverwaltung erfüllen. Die administrativen Ansichten (verwalteten Einheiten) ermöglichen eine verteilte Verwaltung unabhängig von der Hierarchie der Organisationseinheiten.

ActiveRoles Server stellt also verwaltete Einheiten bereit: sicherbare, flexible, regelorientierte, administrative Ansichten. Verwaltete Einheiten stellen dynamische virtuelle Sammlungen von Objekten unterschiedlicher Typen dar. Verwaltete Einheiten können beliebige Verzeichnisobjekte einschließen, unabhängig von ihrem Standort im Netzwerk. Daher können Objekte in administrative Ansichten gruppiert werden, die von der auf Organisationseinheiten basierenden Struktur unabhängig sind.

Mit verwalteten Einheiten können Organisationen Organisationseinheitsstrukturen anhand geografischer Gegebenheiten implementieren, ihre Verwaltung jedoch nach funktionalen Kriterien verteilen. Beispielsweise können alle Benutzer in einer bestimmten Abteilung, unabhängig von ihrer Platzierung in unterschiedlichen Organisationseinheiten, zum Delegieren der Zugriffskontrolle und Durchsetzen administrativer Richtlinien in eine einzelne verwaltete Einheit gruppiert werden. Die Mitglieder dieser verwalteten Einheit bleiben dabei in ihren geografisch definierten Organisationseinheiten. Es entstehen keine Auswirkungen auf die Struktur der Organisationseinheiten.

Mit verwalteten Einheiten können Sie ein Unternehmen auf jede Weise strukturieren, ohne die zugrunde liegende Struktur aus Domänen und Organisationseinheiten zu ändern. Verwaltete Einheiten können Verzeichnisobjekte aus unterschiedlichen Domänenstrukturen und Gesamtstrukturen sowie aus anderen verwalteten Einheiten einschließen. Außerdem können unterschiedliche verwaltete Einheiten gemeinsame Mitglieder enthalten. Dank dieser Funktionen können Sie mit verwalteten Einheiten eine Umgebung erstellen, die sicher und leicht zu verwalten ist.

Funktionsweise verwalteter Einheiten

Mitgliedschaftsregeln bestimmen, ob ein Objekt Mitglied einer bestimmten verwalteten Einheit ist. Beispielsweise können Sie eine Mitgliedschaftsregel mit folgendem Inhalt angeben: Alle Benutzer der Organisationseinheit **A**, deren vollständige Namen mit **B** beginnen, gehören zu dieser verwalteten Einheit. Die Mitgliedschaftsregel wird dann als Abfrage implementiert, die die Organisationseinheit **A** nach Benutzern durchsucht, deren vollständige Namen mit **B** beginnen. ActiveRoles Server speichert die Abfrage in den Eigenschaften der verwalteten Einheit und führt sie bei jeder Erstellung oder Aktualisierung einer Liste von Mitgliedern der verwalteten Einheit aus.

Mit ActiveRoles Server können Berechtigungs- und Richtlinieneinstellungen auf der Ebene verwalteter Einheiten angegeben werden. Die Vererbung von Berechtigungs- und Richtlinieneinstellungen von der Ebene verwalteter Einheiten arbeitet nahtlos in der gesamten Active Directory-Umgebung.

Wenn die Umgebung geändert wird, werden auch die Mitgliedschaften von Objekten in verwalteten Einheiten gemäß der neuen Umgebung automatisch geändert. Dabei werden auch Berechtigungs- und Richtlinieneinstellungen für Objekte geändert. Verwaltete Einheiten werden dynamisch an Änderungen im Unternehmen angepasst. Dies vereinfacht die Verwaltung von Berechtigungs- und Richtlinieneinstellungen für Verzeichnisobjekte.

Jede verwaltetet Einheit stellt einen benutzerfreundlichen Bereich für die delegierte Verwaltung bereit. Delegierte Administratoren müssen nicht die Hierarchie der Organisationseinheiten nach verwalteten Objekten durchsuchen. Mit ActiveRoles Server kann die administrative Kontrolle über jede verwaltete Einheit an bestimmte Benutzer und Gruppen delegiert werden, genau wie die Kontrolle über Organisationseinheiten. Mit verwalteten Einheiten befinden sich alle Objekte, die ein delegierter Administrator verwaltet, an einem einzigen Ort.

Administration verwalteter Einheiten

In diesem Abschnitt wird die Administration verwalteter Einheiten mit der ActiveRoles Server-Konsole vorgestellt. Die folgenden Themen werden behandelt:

- Erstellen einer verwalteten Einheit
- Anzeigen der Mitglieder einer verwalteten Einheit
- Hinzufügen und Entfernen von Mitgliedern einer verwalteten Einheit
- Kopieren einer verwalteten Einheit
- Exportieren und Importieren verwalteter Einheiten
- Umbenennen einer verwalteten Einheit
- Löschen einer verwalteten Einheit

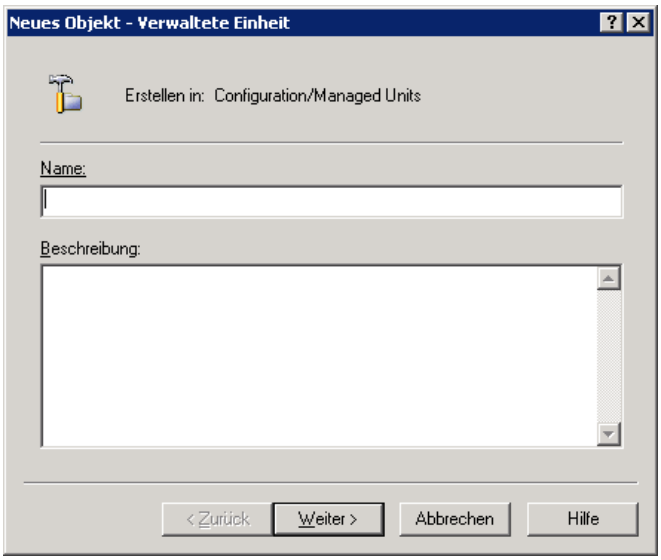
Erstellen einer verwalteten Einheit

Die ActiveRoles Server-Konsole stellt den Assistenten unter „Neues Objekt – verwaltete Einheit" für die Erstellung verwalteter Einheiten bereit. Sie können den Assistenten vom Container **Managed Units** aus starten. Dieser befindet sich in der Konsolenstruktur unter **Konfiguration**: Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf **Managed Units** und wählen Sie **Neu | Verwaltete Einheit** aus.

Für die Administration einer großen Anzahl verwalteter Einheiten sollten Sie wie folgt Container erstellen, die nur angegebene verwaltete Einheiten enthalten, damit Sie sie leicht finden können: Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf **Managed Units** und wählen Sie **Neu | Container für verwaltete Einheit**. Verwenden Sie dann den Assistenten, um eine verwaltete Einheit in diesem Container zu erstellen: Klicken Sie mit der rechten Maustaste auf den Container und klicken Sie dann auf **Neu | Verwaltete Einheit**.

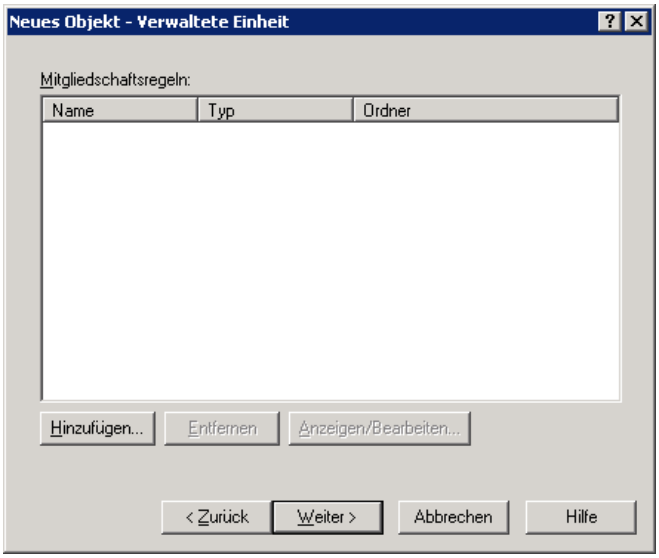
Nur Benutzer mit Administratorzugriff auf den Verwaltungsdienst (Mitglieder des AR Server Admin-Kontos) dürfen verwaltete Einheiten erstellen. Weitere Informationen über das AR Server Admin-Konto finden Sie im ActiveRoles Server – Erste Schritte.

Die erste Seite des Assistenten entspricht der folgenden Abbildung.



Geben Sie auf dieser Seite den Namen und die Beschreibung für die verwaltete Einheit ein. Auf der ActiveRoles Server-Konsole werden im Bereich „Details" in der Liste der verwalteten Einheiten der Name und die Beschreibung angezeigt.

Klicken Sie auf **Weiter**. Die zweite Seite des Assistenten ähnelt der folgenden Abbildung.

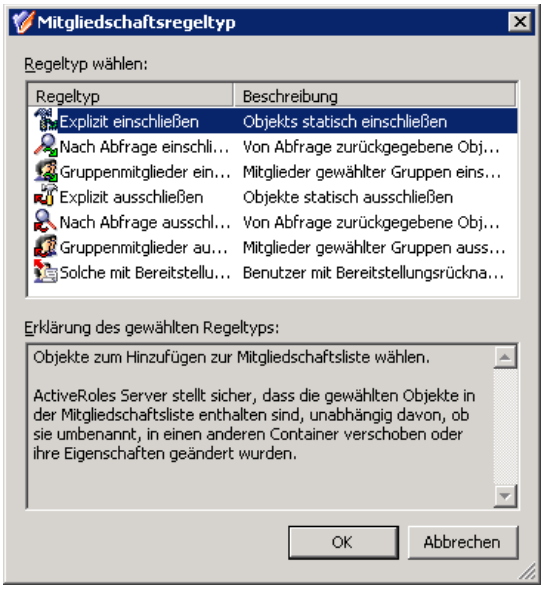


Auf dieser Seite können Sie angeben, welche Objekte in die verwaltete Einheit eingeschlossen werden sollen.

Die Mitgliedschaft in einer verwalteten Einheit wird durch Mitgliedschaftsregeln bestimmt. Mitglieder einer verwalteten Einheit sind die Objekte, die den in den Mitgliedschaftsregeln definierten Kriterien entsprechen. Eine Mitgliederliste kann dynamisch aktualisiert werden: Wenn Sie ein neues Objekt erstellen, das die Kriterien in der Mitgliedschaftsregel erfüllt, wird das Objekt automatisch in die verwaltete Einheit eingeschlossen. Wenn ein Objekt die in der Mitgliedschaftsregel angegebenen Kriterien nicht mehr erfüllt (weil es beispielsweise umbenannt oder verschoben wurde), wird es automatisch aus der Mitgliedschaftsliste ausgeschlossen.

Eine Mitgliedschaftsregel kann die Form einer Suchabfrage, einer Regel für die statische Einschließung und Ausschließung von Objekten sowie einer Regel für die Einschließung und Ausschließung von Gruppenmitgliedern haben.

Klicken Sie zum Angeben einer Mitgliedschaftsregel auf **Hinzufügen**. Hierdurch wird das Dialogfeld **Mitgliedschaftsregeltyp** angezeigt, das in der folgenden Abbildung dargestellt ist.



Wählen Sie in diesem Dialogfeld einen Typ von Mitgliedschaftsregel aus. Im unteren Feld finden Sie eine Beschreibung, die erläutert, welche Mitgliedschaftsregeln mit dem ausgewählten Typ erstellt werden können.

Der Regeltyp **Explizit einschließen** ermöglicht Ihnen, Objekte auszuwählen, die der verwalteten Einheit statisch hinzugefügt werden sollen. Wenn Sie einen Container (z.B. eine Organisationseinheit) auswählen, wird die gesamte Teilstruktur, deren Wurzel dieser Container ist, in die verwaltete Einheit eingeschlossen. ActiveRoles Server stellt sicher, dass die ausgewählten Objekte auch dann in die verwaltete Einheit eingeschlossen sind, wenn sie umbenannt oder in einen anderen Container verschoben werden oder wenn ihre Eigenschaften geändert werden.

Der Regeltyp **Explizit ausschließen** ermöglicht Ihnen, Objekte auszuwählen, die aus der verwalteten Einheit statisch ausgeschlossen werden sollen. ActiveRoles Server stellt sicher, dass die ausgewählten Objekte auch dann aus der Mitgliedschaftsliste ausgeschlossen sind, wenn sie umbenannt oder verschoben werden oder wenn ihre Eigenschaften geändert werden. Da die Regel **Explizit ausschließen** Vorrang vor allen anderen Regeltypen hat, werden die ausgewählten Objekte auch dann aus der verwalteten Einheit ausgeschlossen, wenn eine andere Regel besagt, dass sie eingeschlossen werden sollen.

Mit dem Regeltyp **Gruppenmitglieder einschließen** können Sie die Gruppen auswählen, deren Mitglieder Sie in die verwaltete Einheit einschließen möchten. ActiveRoles Server füllt die Mitgliedschaftsliste dynamisch mit den Objekten auf, die den ausgewählten Gruppen angehören. Wenn ein Objekt den ausgewählten Gruppen hinzugefügt oder aus ihnen entfernt wird, fügt ActiveRoles Server dieses Objekt der Mitgliedschaftsliste der verwalteten Einheit hinzu bzw. entfernt es aus ihr.

Mit dem Regeltyp **Gruppenmitglieder ausschließen** können Sie Gruppen auswählen, deren Mitglieder aus der verwalteten Einheit ausgeschlossen werden sollen. ActiveRoles Server stellt sicher, dass die Mitglieder der ausgewählten Gruppen aus der Mitgliedschaftsliste der verwalteten Einheit entfernt werden. Wenn ein Objekt einer der ausgewählten Gruppen hinzugefügt wird, entfernt ActiveRoles Server dieses Objekt automatisch aus der Mitgliedschaftsliste.

Mit dem Regeltyp **Nach Abfrage einschließen** können Sie Kriterien definieren, die die Objekte erfüllen müssen, um in die verwaltete Einheit eingeschlossen zu werden. ActiveRoles Server füllt die Mitgliedschaftsliste dynamisch mit den Objekten auf, die bestimmte Eigenschaften aufweisen. Wenn ein Objekt erstellt wird oder wenn seine Eigenschaften geändert werden, fügt ActiveRoles Server dieses Objekt der Mitgliedschaftsliste hinzu bzw. entfernt es daraus, abhängig davon, ob die Eigenschaften des Objekts den definierten Kriterien entsprechen.

Mit dem Regeltyp **Nach Abfrage ausschließen** können Sie Kriterien definieren, die die Objekte erfüllen müssen, um aus der verwalteten Einheit ausgeschlossen zu werden. ActiveRoles Server stellt sicher, dass Objekte mit bestimmten Eigenschaften aus der Mitgliedschaftsliste ausgeschlossen werden. ActiveRoles Server entfernt Objekte abhängig davon, ob die Eigenschaften der Objekte den definierten Kriterien entsprechen, automatisch aus der Mitgliedschaftsliste.

Die Regel **Solche mit Bereitstellungsrücknahme beibehalten** dient zur Anpassung des Verhaltens verwalteter Einheiten in Bezug auf deprovisionierte Objekte wie etwa deprovisioniert Benutzer oder Gruppen. Nach der Deprovision eines Objekts wird das Objekt standardmäßig automatisch aus allen verwalteten Einheiten entfernt, in denen es Mitglied war. Wenn es notwendig ist, deprovisionierte Objekte in bestimmten verwalteten Einheiten beizubehalten, fügen Sie diesen verwalteten Einheiten die Regel **Deprovisioniert beibehalten** hinzu. Diese Regel führt dazu, dass die verwaltete Einheit sowohl die normalen als auch die deprovisionierten Objekte enthält, die den Mitgliedschaftsregeln für diese verwaltete Einheit entsprechen. Ohne diese Regel enthält die verwaltete Einheit keine deprovisionierten Objekte.

Wählen Sie im Dialogfeld **Mitgliedschaftsregeltyp** einen Regeltyp aus und klicken Sie auf **OK**.

Wenn Sie den Regeltyp **Explizit einschließen** oder **Explizit ausschließen** ausgewählt haben, wird das Dialogfeld **Objekte auswählen** angezeigt. Wählen Sie die Objekte aus, die Sie in die verwaltete Einheit einschließen oder aus ihr ausschließen möchten, klicken Sie auf **Hinzufügen** und klicken Sie dann auf **OK**.

Wenn Sie den Regeltyp **Gruppenmitglieder einschließen** oder **Gruppenmitglieder ausschließen** ausgewählt haben, wird das Dialogfeld **Objekte auswählen** angezeigt. Die Liste der Objekte in diesem Dialogfeld besteht aus Gruppen. Wählen Sie Gruppen aus, klicken Sie auf **Hinzufügen** und dann auf **OK**. Alle Mitglieder der ausgewählten Gruppen werden in die verwaltete Einheit eingeschlossen oder aus ihr ausgeschlossen.

Wenn Sie den Regeltyp **Nach Abfrage einschließen** oder **Nach Abfrage ausschließen** ausgewählt haben, wird das Dialogfeld **Mitgliedschaftsregel erstellen** angezeigt, das dem Dialogfeld **Suchen** ähnelt. Definieren Sie in diesem Dialogfeld die Kriterien, die Objekte erfüllen müssen, um in die verwaltete Einheit eingeschlossen oder aus ihr ausgeschlossen zu werden.

Nach dem Hinzufügen einer Mitgliedschaftsregel können Sie weitere Mitgliedschaftsregeln für dieselbe verwaltete Einheit hinzufügen.

Wenn Sie der verwalteten Einheit mehrere Mitgliedschaftsregeln hinzufügen und einige davon miteinander in Konflikt stehen, wird der Konflikt durch eine Regel gelöst, die die folgende Rangordnung definiert:

1. Explizit ausschließen
2. Explizit einschließen
3. Nach Abfrage ausschließen
4. Gruppenmitglieder ausschließen
5. Nach Abfrage einschließen
6. Gruppenmitglieder einschließen

Nach dieser Rangfolge hat z.B. die Regel **Explizit ausschließen** Vorrang vor allen anderen Regeltypen. Daher werden die ausgewählten Objekte auch dann aus der verwalteten Einheit ausgeschlossen, wenn eine andere Regel angibt, dass sie eingeschlossen werden sollen (beispielsweise die Objekte, die die in der Mitgliedschaftsregel **Nach Abfrage einschließen** definierten Kriterien erfüllen, oder zu einer Gruppe gehören, die in der Regel **Gruppenmitglieder einschließen** ausgewählt wurde).

Klicken Sie nach dem Auswählen von Mitgliedschaftsregeln auf **Weiter**. Die folgende Seite wird angezeigt:

Auf dieser Seite können Sie die Berechtigungs- und Richtlinieneinstellungen für die verwaltete Einheit angeben. Klicken Sie nach Abschluss des Vorgangs auf **Weiter** und dann auf **Fertig stellen**. Informationen über Berechtigungseinstellungen finden Sie unter „Anwenden von Zugriffsvorlagen" weiter oben in diesem Dokument. Informationen über Richtlinieneinstellungen finden Sie unter „Anwenden von Richtlinienobjekten" weiter oben in diesem Dokument.

Schrittweise Anleitungen bezüglich der Festlegung von Berechtigungs- und Richtlinieneinstellungen für eine verwaltete Einheit finden Sie in den Themen **Ändern der Berechtigungseinstellungen für eine verwaltete Einheit** und **Ändern der Richtlinieneinstellungen für eine verwaltete Einheit** unter der Überschrift **Anleitungen/Administration verwalteter Einheiten** in der ActiveRoles Server-Hilfe.

Schrittweise Anleitungen bezüglich der Erstellung einer verwalteten Einheit finden Sie unter **Anleitungen/Administration verwalteter Einheiten/Erstellen einer verwalteten Einheit** in der ActiveRoles Server-Hilfe.

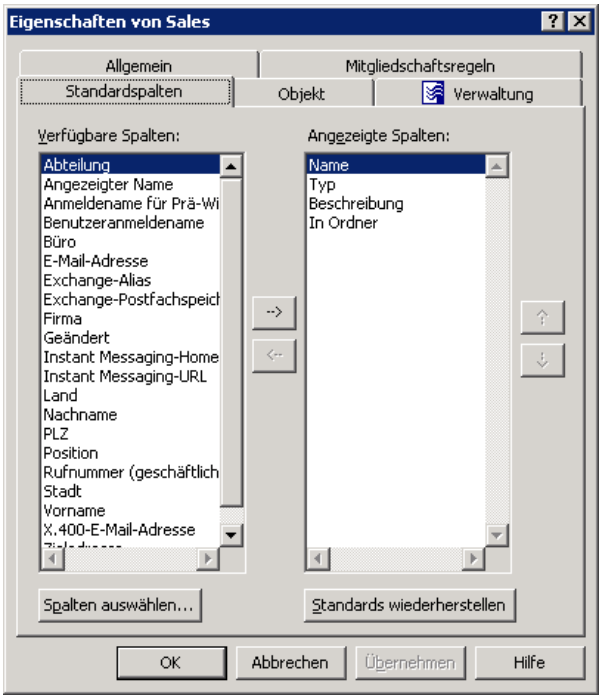
Anzeigen der Mitglieder einer verwalteten Einheit

Die Mitglieder einer verwalteten Einheit sind Objekte, die den Kriterien entsprechen, die in den Mitgliedschaftsregeln für die verwaltete Einheit angegeben sind.

Um die Mitglieder einer verwalteten Einheit anzuzeigen, erweitern Sie in der Konsolenstruktur **Configuration/Managed Units** und klicken Sie dann auf eine verwaltete Einheit. Im Bereich „Details" werden nun die Mitglieder der verwalteten Einheit angezeigt.

Sie können für jede verwaltete Einheit eine eigene Spaltengruppe vorher festlegen, die im Bereich „Details" angezeigt werden soll. So können Sie administrative Ansichten für einzelne verwaltete Einheiten festlegen.

Um für eine bestimmte verwaltete Einheit Spalten im Bereich „Details" vorher festzulegen, klicken Sie mit der rechten Maustaste auf die verwaltete Einheit, klicken Sie auf **Eigenschaften**, und öffnen Sie die Registerkarte **Standardspalten**. Die Registerkarte ähnelt der folgenden Abbildung:



Um eine anzuzeigende Spalte hinzuzufügen, doppelklicken Sie in der Liste **Verfügbare Spalten** auf ihren Namen. Um Spalten zur Liste **Verfügbare Spalten** hinzuzufügen, klicken Sie auf **Spalten auswählen**. Im Dialogfeld **Spalten auswählen** können Sie Spalten auswählen und erforderlichenfalls die Namen ändern, die in den Spaltenüberschriften angezeigt werden.

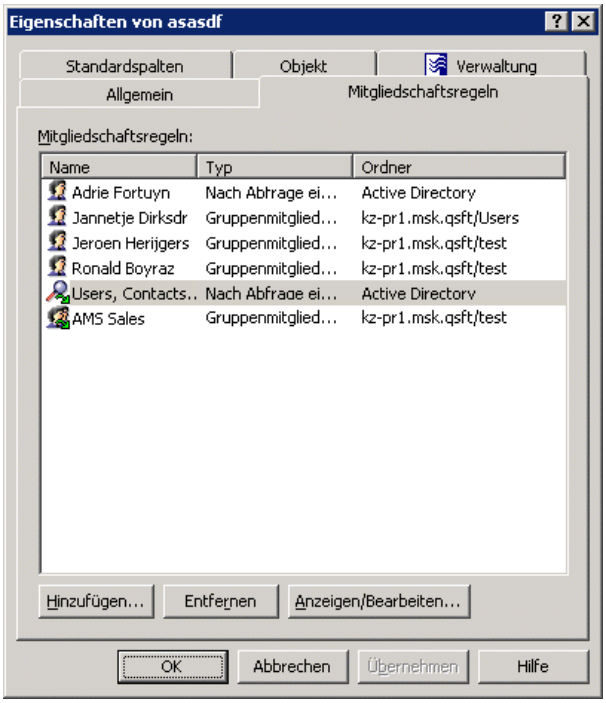
Durch Doppelklicken auf einen Spaltennamen unter **Verfügbare Spalten** wird der Name zur Liste **Angezeigte Spalten** hinzugefügt. Klicken Sie auf **OK**. Die neue Spalte wird nach dem Aktualisieren der Ansicht im Bereich „Details" angezeigt. Klicken Sie mit der rechten Maustaste in der Konsolenstruktur auf **Managed Units** und klicken Sie dann auf **Aktualisieren**; wählen Sie dann die verwaltete Einheit in der Konsolenstruktur aus: Im Bereich „Details" wird die neue Spalte angezeigt.

Schrittweise Anleitungen bezüglich der Anzeige von Mitgliedern einer verwalteten Einheit und der Anpassung der Ansicht einer verwalteten Einheit finden Sie unter **Anleitungen/Administration verwalteter Einheiten/Mitglieder einer verwalteten Einheit anzeigen** in der ActiveRoles Server-Hilfe.

Hinzufügen und Entfernen von Mitgliedern einer verwalteten Einheit

Die Mitglieder einer verwalteten Einheit werden durch Mitgliedschaftsregeln definiert. Zum Hinzufügen oder Entfernen von Mitgliedern einer verwalteten Einheit müssen Sie daher Mitgliedschaftsregeln hinzufügen, löschen oder ändern.

Zeigen Sie dazu das Dialogfeld **Eigenschaften** für die entsprechende verwaltete Einheit an und klicken Sie dann auf die Registerkarte **Mitgliedschaftsregeln**. Die Registerkarte ähnelt der folgenden Abbildung:



Auf der Registerkarte **Mitgliedschaftsregeln** wird eine Liste von Mitgliedschaftsregeln angezeigt. Dabei zeigt jeder Eintrag den Namen, Typ und Gültigkeitsbereich der Regel an.

Klicken Sie zum Hinzufügen einer Mitgliedschaftsregel auf **Hinzufügen**. Hierdurch wird das Dialogfeld **Mitgliedschaftsregeltyp** geöffnet, das weiter oben in diesem Kapitel beschrieben wurde (siehe „Erstellen einer verwalteten Einheit").

Um eine Mitgliedschaftsregel zu ändern, wählen Sie sie in der Liste **Mitgliedschaftsregeln** aus und klicken Sie dann auf **Anzeigen/Bearbeiten**. Nur abfragebasierte Regeln können auf diese Weise geändert werden. Wenn Sie eine Regel eines anderen Typs auswählen, ist die Schaltfläche **Anzeigen/Bearbeiten** nicht verfügbar.

Um eine Mitgliedschaftsregel zu löschen, wählen Sie sie in der Liste **Mitgliedschaftsregeln** aus, und klicken Sie dann auf **Entfernen**.

Wenn Sie Mitgliedschaftsregeln hinzufügen, ändern oder löschen, wird auch die Mitgliedschaftsliste der verwalteten Einheit geändert.

Schrittweise Anleitungen bezüglich des Hinzufügens von Mitgliedschaftsregeln zu bzw. des Entfernens von Mitgliedschaftsregeln aus einer verwalteten Einheit finden Sie in den entsprechenden Themen unter der Überschrift **Anleitungen/Administration verwalteter Einheiten** in der ActiveRoles Server-Hilfe.

Kopieren einer verwalteten Einheit

Mit der ActiveRoles Server-Konsole können Sie Kopien verwalteter Einheiten erstellen. Mit dieser Funktion können Sie vorhandene verwaltete Einheiten wieder verwenden.

Um eine Kopie einer verwalteten Einheit zu erstellen, klicken Sie mit der rechten Maustaste auf die verwaltete Einheit und klicken Sie dann auf **Kopieren**. Hierdurch wird der Assistent „Objekt kopieren – Verwaltete Einheit" geöffnet. Sie können den Assistenten abschließen, indem Sie die Anweisungen im Abschnitt „Erstellen einer verwalteten Einheit" weiter oben in diesem Kapitel befolgen.

Schrittweise Anleitungen bezüglich der Erstellung einer Kopie einer verwalteten Einheit finden Sie unter **Anleitungen/Administration verwalteter Einheiten/Kopieren einer verwalteten Einheit** in der ActiveRoles Server-Hilfe.

Exportieren und Importieren einer verwalteten Einheit

Mit der ActiveRoles Server-Konsole können Sie verwaltete Einheiten in eine XML-Datei exportieren und sie dann aus dieser Datei importieren, um eine andere Instanz von ActiveRoles Server aufzufüllen. Die Export- und Importvorgänge stellen eine Möglichkeit bereit, verwaltete Einheiten von einer Testumgebung in eine Produktionsumgebung zu verschieben.

Wenn Sie eine verwaltete Einheit exportieren und dann importieren, werden nur Mitgliedschaftsregeln zusammen mit anderen Eigenschaften der verwalteten Einheit übertragen. Die Berechtigungs- und Richtlinieneinstellungen für die verwaltete Einheit werden nicht in den Export-Import-Vorgang eingeschlossen. Sie müssen sie nach Abschluss des Vorgangs manuell neu konfigurieren.

Um verwaltete Einheiten zu exportieren, wählen Sie sie aus, klicken Sie mit der rechten Maustaste auf die Auswahl und wählen Sie dann **Alle Aufgaben | Exportieren**. Geben Sie im Dialogfeld **Objekte exportieren** die Datei an, in der Sie die Daten speichern möchten, und klicken Sie dann auf **Speichern**.

Zum Importieren verwalteter Einheiten klicken Sie mit der rechten Maustaste auf den Container, in dem Sie die verwalteten Einheiten ablegen möchten, und klicken Sie dann auf **Importieren**. Wählen Sie im Dialogfeld **Verzeichnisobjekte importieren** die Datei aus, in die die verwalteten Einheiten exportiert wurden, und klicken Sie dann auf **Öffnen**.

Schrittweise Anleitungen bezüglich des Exports und Imports von verwalteten Einheiten finden Sie in den Themen **Exportieren einer verwalteten Einheit** und **Importieren einer verwalteten Einheit** unter **Anleitungen/Administration verwalteter Einheiten** in der ActiveRoles Server-Hilfe.

Umbenennen einer verwalteten Einheit

Um eine verwaltete Einheit umzubenennen, klicken Sie mit der rechten Maustaste auf die verwaltete Einheit und klicken dann auf **Umbenennen**. Geben Sie den neuen Namen ein und drücken Sie dann die Eingabetaste.

Das Umbenennen einer verwalteten Einheit hat keine Auswirkungen auf die Mitgliedschaftsregeln, Berechtigungseinstellungen oder Richtlinieneinstellungen, die der verwalteten Einheit zugeordnet sind.

Schrittweise Anleitungen bezüglich der Umbenennung einer verwalteten Einheit finden Sie unter **Anleitungen/Administration verwalteter Einheiten/Umbenennen einer verwalteten Einheit** in der ActiveRoles Server-Hilfe.

Löschen einer verwalteten Einheit

Um eine verwaltete Einheit zu löschen, klicken Sie mit der rechten Maustaste auf die verwaltete Einheit und klicken dann auf **Löschen**.

Wenn Sie eine verwaltete Einheit löschen, werden die darin enthaltenen Objekte nicht gelöscht. Der Löschvorgang löscht die Mitgliedschaftsregeln, Berechtigungseinstellungen und Richtlinieneinstellungen, die der verwalteten Einheit zugeordnet sind.

Schrittweise Anleitungen bezüglich des Löschens einer verwalteten Einheit finden Sie unter **Anleitungen/Administration verwalteter Einheiten/Löschen einer verwalteten Einheit** in der ActiveRoles Server-Hilfe.

Szenario: Implementieren der rollenbasierten Verwaltung über mehrere Organisationseinheiten hinweg

In diesem Szenario wird eine administrative Ansicht mit dem Namen **Vertrieb** erstellt. Sie befindet sich in einer Organisation mit der Active Directory-Struktur, die auf Organisationseinheiten basiert.

Angenommen, eine Organisation verfügt über Niederlassungen in den USA und Kanada. Die Regel für das Einschließen eines Benutzers in eine Organisationseinheit ist der geografische Standort des Benutzers. Daher befinden sich alle Benutzer, die in den USA arbeiten, in der Organisationseinheit **USA**, und die, die in Kanada arbeiten, befinden sich in der Organisationseinheit **Kanada**.

Die Büros in den USA und in Kanada haben jeweils eine **Marketing-**, **Entwicklungs-** und **Vertriebsabteilung**. Indem Sie die verwaltete Einheit **Vertrieb** erstellen, können Sie Benutzer aus den **Vertriebsabteilungen** in den USA und Kanada gemeinsam verwalten, ohne die eigentliche, auf Organisationseinheiten basierende Struktur zu ändern.

Beim Delegieren der Kontrolle über eine verwaltete Einheit erben alle Benutzer in dieser verwalteten Einheit Sicherheitseinstellungen, die auf der Ebene der verwalteten Einheit definiert sind. Daher werden beim Anwenden einer Zugriffsvorlage auf eine verwaltete Einheit die Sicherheitseinstellungen für jeden Benutzer in der verwalteten Einheit festgelegt.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen Sie die verwaltete Einheit **Vertrieb**.
2. Fügen Sie Benutzer aus den **Vertriebsabteilungen** in den USA und Kanada zur verwalteten Einheit **Vertrieb** hinzu.
3. Bereiten Sie die Zugriffsvorlage **Sales** vor.
4. Wenden Sie die Zugriffsvorlage **Sales** auf die verwaltete Einheit **Vertrieb** an und wählen Sie eine geeignete Gruppe als Trustee aus.

Folglich erhalten die Mitglieder der Gruppe Kontrolle über Benutzerkonten, die der verwalteten Einheit **Vertrieb** angehören. Der Bereich der Kontrolle wird durch die Berechtigungen in der Zugriffsvorlage **Sales** definiert.

In den folgenden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen der verwalteten Einheit

Im ersten Schritt erstellen Sie die verwaltete Einheit **Vertrieb**. Informationen über die Erstellung einer verwalteten Einheit finden Sie unter „Erstellen einer verwalteten Einheit" weiter oben in diesem Kapitel.

Schritt 2: Hinzufügen von Benutzern zu der verwalteten Einheit

Nach dem Vorbereiten der verwalteten Einheit **Vertrieb** fügen Sie ihre Benutzer aus den **Vertriebsabteilungen** im gesamten Unternehmen hinzu.

Nehmen Sie an, dass für alle Benutzer in den **Vertriebsabteilungen** (in den USA und in Kanada) die Eigenschaft **Beschreibung** auf **Vertrieb** festgelegt ist.

Erstellen Sie eine Mitgliedschaftsregel vom Typ **Nach Abfrage einschließen** mit folgenden Parametern: Wählen Sie aus der Liste **Suchen** die Option **Benutzer** aus. Geben Sie in das Feld **Beschreibung** den Wert **Vertrieb** ein. Somit werden alle Benutzer mit der Beschreibung **Vertrieb** in die verwaltete Einheit eingeschlossen.

Weitere Informationen über die Erstellung von Mitgliedschaftsregeln finden Sie unter „Hinzufügen und Entfernen von Mitgliedern einer verwalteten Einheit" weiter oben in diesem Kapitel.

Schritt 3: Vorbereiten der Zugriffsvorlage

Um die Rechte des Trustees für die verwaltete Einheit **Vertrieb** zu definieren, erstellen Sie die Zugriffsvorlage **Sales** und fügen Sie ihr Berechtigungen hinzu.

Weitere Informationen über die Erstellung einer Zugriffsvorlage finden Sie unter „Erstellen von Zugriffsvorlagen" weiter oben in diesem Dokument.

Schritt 4: Anwenden der Zugriffsvorlage

Um die Zugriffsvorlage **Sales** auf die verwaltete Einheit **Vertrieb** anzuwenden, klicken Sie mit der rechten Maustaste auf die verwaltete Einheit **Vertrieb** und klicken Sie auf **Kontrolle delegieren**. Klicken Sie dann auf die Schaltfläche **Hinzufügen** und befolgen Sie die Anleitungen im Assistenten „Delegation der Kontrolle".

Fügen Sie auf der Seite **Benutzer oder Gruppen** des Assistenten den Benutzer oder die Gruppe hinzu, der bzw. die als Trustee ausgewählt werden sollen.

Wählen Sie auf der Seite **Zugriffsvorlagen** des Assistenten die Zugriffsvorlage **Sales** aus, die Sie in Schritt 3 vorbereitet haben.

Weitere Informationen über die Anwendung einer Zugriffsvorlage auf eine verwaltete Einheit finden Sie unter „Anwenden von Zugriffsvorlagen" weiter oben in diesem Dokument.

4

Rollenbasierte Administration

- Zugriffsvorlagen zum Definieren von Administratorfunktionen
- Verwaltungsaufgaben für Zugriffsvorlagen
- Verwendungsbeispiele

Zugriffsvorlagen zum Definieren von Administratorfunktionen

ActiveRoles Server stellt eine sichere, verteilte Verwaltung über die erweiterte Delegierung von Rechten mit sehr hoher Granularität an einzelne Benutzer oder Gruppen sicher. Dies nimmt hoch qualifizierten Administratoren tägliche Routineaufgaben ab und spart ihnen Zeit, sodass ihre Produktivität erhöht wird. Beispielsweise kann ein Administrator dem Help Desk die Ausführung bestimmter Aufgaben (z.B. das Zurücksetzen von Kennwörtern oder das Verwalten von Gruppenmitgliedschaften) gestatten, ohne den Help Deskmitarbeitern vollständige Administratorrechte zu erteilen.

Beim Entwickeln des Verwaltungs- und Sicherheitsentwurfs definieren Sie delegierte Administratoren (Trustees) sowie Administratorfunktionen (Zugriffsvorlagen). Dann definieren Sie verwaltete Einheiten und wenden Zugriffsvorlagen an, wobei Sie für jede verwaltete Einheit Trustees auswählen. Sie können Zugriffsvorlagen auch auf Objekte und Ordner in Active Directory anwenden und so die Berechtigungen den erforderlichen Trustees zuweisen. Diese dreiseitige Beziehung zwischen Trustees, Zugriffsvorlagen und verwalteten Objekten ist für die Implementierung Ihres rollenbasierten Verwaltungsmodells zentral.

Das Tool „Benutzer und Computer" von Active Directory ermöglicht die Delegierung von Administrator-verantwortlichkeiten. Sie müssen allerdings bei jeder Delegierung von Rechten eine Gruppe von Berechtigungen definieren. Dadurch wird der Delegierungsvorgang zeitaufwändig und fehleranfällig. ActiveRoles Server löst dieses Problem durch Konsolidierung von Berechtigungen in anpassbare Administratorfunktionen – Zugriffsvorlagen. Die logische Gruppierung von Berechtigungen vereinfacht die Verwaltung von Delegierungseinstellungen.

Zugriffsvorlagen sind Sammlungen von Berechtigungen, die Administratorfunktionen darstellen. Berechtigungen werden verwendet, um einem Benutzer oder einer Gruppe bestimmte administrative Vorgänge zu gestatten oder zu verbieten. Sie können eine Zugriffsvorlage erstellen, die alle erforderlichen Berechtigungen für die Ausführung einer bestimmten Administratorfunktion enthalten.

Um einem Benutzer oder einer Gruppe die Funktion zuzuweisen, sollten Sie die Zugriffsvorlage je nach dem Gültigkeitsbereich der Funktion mit einer verwalteten Einheit, einer Organisationseinheit, einer Domäne oder einem einzelnen Objekt verknüpfen und dann einen Benutzer oder eine Gruppe als Trustee auswählen. Infolgedessen erhält der einzelne Benutzer bzw. jedes Mitglied der Gruppe die durch die Funktion angegebenen Rechte zum Verwalten von Objekten in der Auflistung oder dem Ordner, mit der bzw. dem die Zugriffsvorlage verknüpft wurde.

Funktionsweise von Zugriffsvorlagen

ActiveRoles Server implementiert die delegierte Verwaltung durch Verknüpfen von Zugriffsvorlagen mit Objektauflistungen (verwalteten Einheiten), Verzeichnisordnern (Containern) oder einzelnen Objekten (Blattobjekten).

Bei Anwendung auf ein Verzeichnisobjekt gibt eine Zugriffsvorlage Berechtigungseinstellungen für dieses Objekt und seine untergeordneten Objekte an. Durch Anwenden von Zugriffsvorlagen auf verwaltete Einheiten können Berechtigungen für Auflistungen von Verzeichnisobjekten bequem verwaltet werden.

Jede Zugriffsvorlage wird in Bezug auf einige Benutzer und/oder Gruppen (Trustees) angewendet, und die in der Zugriffsvorlage festgelegten Berechtigungen bestimmen ihren Zugriff auf verwaltete Objekte. Wenn eine Zugriffsvorlage verändert oder nicht mehr angewendet wird, werden die für die Verzeichnisobjekte festgelegten Berechtigungen entsprechend geändert.

Wenn Berechtigungen für eine verwaltete Einheit geändert werden, berechnet ActiveRoles Server die Berechtigungseinstellungen für alle Mitglieder der verwalteten Einheit neu. Ebenso werden die Berechtigungsinformationen geändert, wenn die Liste der Objekte in einer verwalteten Einheit geändert wird. Wenn Objekte der verwalteten Einheit hinzugefügt oder aus ihr entfernt werden (beispielsweise aufgrund von Änderungen an Objekteigenschaften), werden alle Berechtigungseinstellungen für diese Objekte neu berechnet.

Jedes Objekt erbt seine Berechtigungseinstellungen von den verwalteten Einheiten, in denen es sich befindet. Wenn ein Trustee beispielsweise über Zugriffsberechtigungen für mehrere verwaltete Einheiten verfügt, die ein bestimmtes Objekt enthalten, sind die Zugriffsberechtigungen des Trustees für dieses Objekt einfach als Vereinigung aller Berechtigungen definiert, die auf der Ebene der verwalteten Einheiten angegeben sind.

Bei der Anwendung von Zugriffsvorlagen auf ein Containerobjekt (einen Verzeichnisordner) wird der Zugriff des Trustees auf den Container und seine untergeordneten Objekte eingerichtet. Durch die angegebenen Berechtigungen für einen Container verfügt der Trustee auch über vererbte Berechtigungen für die untergeordneten Objekte in dem Container.

Sicherheitssynchronisierung

In einer Zugriffsvorlage definierte Berechtigungen können an Active Directory weitergegeben werden. Dabei werden alle Änderungen, die in ActiveRoles Server an ihnen vorgenommen wurden, automatisch in Active Directory synchronisiert.

Mit Hilfe der Synchronisierung von der ActiveRoles Server-Sicherheit zur einheitlichen Sicherheit von Active Directory ermöglicht ActiveRoles Server das Angeben von Sicherheitseinstellungen für Active Directory über Zugriffsvorlagen. Zugriffsvorlagen vereinfachen und erweitern die Verwaltung von Berechtigungen in Active Directory, ermöglichen die logische Gruppierung von Berechtigungen und stellen einen effizienten Mechanismus für das Festlegen und Aufrechterhalten der Zugriffskontrolle dar.

Für jeden Berechtigungseintrag, der in ActiveRoles Server definiert und mit der Optionengruppe **Berechtigungsweitergabe** konfiguriert ist, generiert ActiveRoles Server einheitliche Berechtigungseinträge von Active Directory auf der Grundlage des Berechtigungseintrags von ActiveRoles Server.

Mit der Option **Berechtigungsweitergabe** (auf der Benutzeroberfläche auch als **Mit einheitlicher Sicherheit synchronisieren** oder **Mit AD synchronisieren** bezeichnet) wird sichergestellt, dass bei jeder Änderung von Berechtigungen in ActiveRoles Server die zugeordneten einheitlichen Berechtigungseinträge entsprechend geändert werden.

Wenn Sie die Option **Berechtigungsweitergabe** für vorhandene ActiveRoles Server-Berechtigungen deaktivieren oder ActiveRoles Server-Berechtigungen deaktivieren, für die diese Option festgelegt ist, werden alle einheitlichen Berechtigungseinträge gelöscht, die durch diese ActiveRoles Server-Berechtigungen angegeben werden.

Wenn ein weitergegebener Berechtigungseintrag absichtlich oder versehentlich aus Active Directory gelöscht oder in Active Directory geändert wird, stellt ActiveRoles Server diesen Eintrag anhand der Informationen in der Zugriffsvorlage wieder her und stellt so sicher, dass in Active Directory die richtigen Berechtigungseinstellungen vorhanden sind. Die geplante Aufgabe „Synchronisation von Berechtigungen für Active Directory" wird in ActiveRoles Server verwendet, um Berechtigungseinträge in Active Directory auf der Grundlage der Zugriffsvorlagenverknüpfungen, für die die Option „Berechtigungsverbreitung" aktiviert ist, zu erstellen oder zu aktualisieren.

Verwaltungsaufgaben für Zugriffsvorlagen

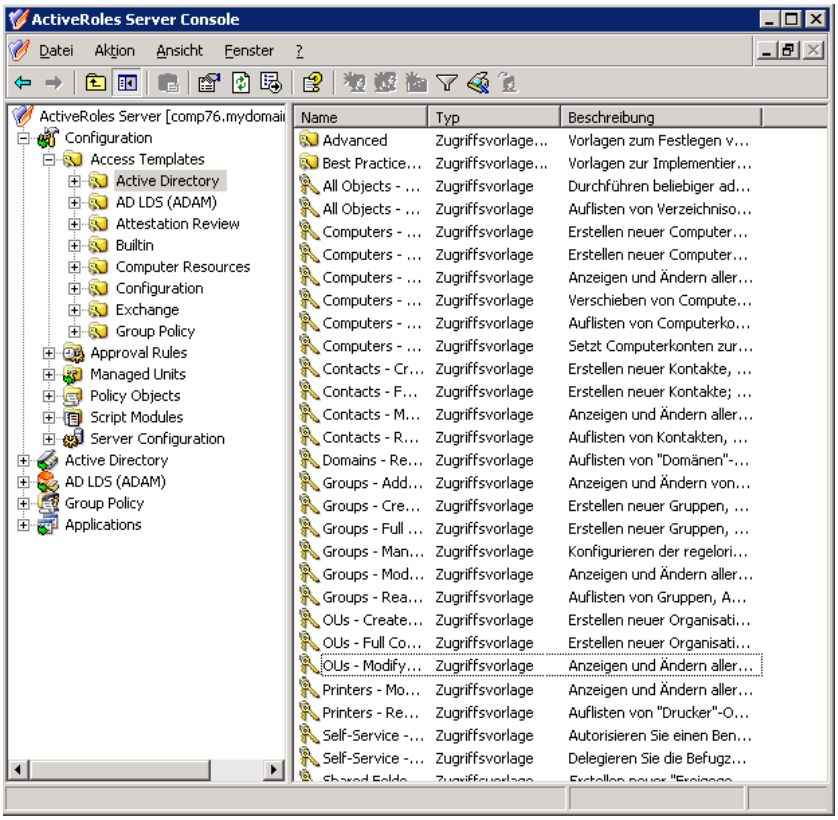
In diesem Abschnitt wird die Verwaltung von Zugriffsvorlagen mit der ActiveRoles Server-Konsole vorgestellt. Die folgenden Themen werden behandelt:

- Verwenden vordefinierter Zugriffsvorlagen
- Erstellen einer Zugriffsvorlage
- Anwenden von Zugriffsvorlagen
- Verwalten von Zugriffsvorlagenverknüpfungen
- Synchronisieren von Berechtigungen nach Active Directory
- Hinzufügen, Ändern und Entfernen von Berechtigungen
- Schachteln von Zugriffsvorlagen
- Kopieren von Zugriffsvorlagen
- Exportieren und Importieren von Zugriffsvorlagen
- Umbenennen einer Zugriffsvorlage
- Löschen einer Zugriffsvorlage

Verwenden vordefinierter Zugriffsvorlagen

ActiveRoles Server bietet eine umfangreiche Suite vordefinierter Zugriffsvorlagen, die typische Administratorfunktionen darstellen und das schnelle und konsistente Delegieren der richtigen Administratorautoritätsebene ermöglichen.

Die vordefinierten Zugriffsvorlagen befinden sich in Containern unter **Configuration/Access Templates**, wie in der folgenden Abbildung gezeigt.



Sie können im Bereich „Details" eine Liste von Zugriffsvorlagen anzeigen, indem Sie **Configuration | Access Templates** erweitern und einen der folgenden Container in der Konsolenstruktur auswählen:

- Active Directory
- AD LDS (ADAM)
- Attestation Review
- Computer Resources
- Configuration
- Exchange

Active Directory

Sie können Zugriffsvorlagen aus dem Container **Active Directory** verwenden, um Datenverwaltungsaufgaben von Active Directory und Dienstverwaltungsaufgaben von Active Directory zu delegieren, z.B.:

- Benutzer- und Gruppenverwaltung
- Verwaltung von Objekten für Computer, Druckerwarteschlangen oder freigegebene Ordner
- Verwaltung der Gesamtstruktur- und Domänenkonfiguration

Dieser Container enthält Vorlagen für zahlreiche Verwaltungsaufgaben und Vorlagen, die den Zugriff auf ausgewählte Eigenschaften von Active Directory-Objekten einschränken.

AD LDS (ADAM)

Sie können Zugriffsvorlagen aus dem Container **AD LDS (ADAM)** verwenden, um die Datenverwaltungsaufgaben für Microsoft Active Directory Lightweight Directory Services (AD LDS) – einem unabhängigen Modus von Active Directory, zuvor bekannt unter der Bezeichnung „Active Directory Application Mode" (ADAM) – zu delegieren. ActiveRoles Server ermöglicht die selektive Delegation von Aufgaben für AD LDS-Objekte dieser Kategorien:

- AD LDS-Container
- AD LDS-Gruppe
- AD LDS-Organisationseinheit
- AD LDS-Benutzer

Anweisungen bezüglich der Anzeige oder der Festlegung von Berechtigungen für AD LDS-Objekte finden Sie im Kapitel „AD LDS-Datenverwaltung" weiter unten in diesem Dokument.

Attestation Review

Sie können Zugriffsvorlagen aus dem Container **Attestation Review** verwenden, um Aufgaben wie etwa die Konfiguration und den Start von Prüfungen, die Durchführung von Prüfungen und die Analyse der Prüfungsergebnisse, die mit der Funktion „Bestätigungsprüfung" verbunden sind, zu delegieren.

Computer Resources

Mit Zugriffsvorlagen aus dem Container **Computer Resources** können Sie Verwaltungsaufgaben für Ressourcen delegieren, die sich auf lokalen Computern befinden, z.B.:

- Lokale Benutzer und Gruppen
- Dienste
- Netzwerkdateifreigaben (freigegebene Verzeichnisse)
- Drucker und Druckaufträge

Dieser Container enthält Vorlagen für bestimmte Administratorfunktionen (z.B. den Druckeroperator oder den Dienstoperator), sowie Vorlagen, mit denen der Zugriff auf ausgewählte Eigenschaften lokaler Computerressourcen angegeben wird.

Configuration

Mit Zugriffsvorlagen aus dem Container **Configuration** können Sie Verwaltungsaufgaben für die ActiveRoles Server-Konfiguration delegieren, z.B.:

- Administration verwalteter Einheiten, Richtlinienobjekte oder Zugriffsvorlagen
- Konfigurieren der Replikation (Hinzufügen oder Entfernen von Replikationspartnern)
- Hinzufügen oder Entfernen verwalteter Domänen

Dieser Container schließt auch Vorlagen ein, die den Zugriff auf einzelne Eigenschaften von verwalteten Einheiten, Richtlinienobjekten und Zugriffsvorlagen steuern.

Exchange

Mit Zugriffsvorlagen aus dem Container **Exchange** können Sie die folgenden Verwaltungsaufgaben für Exchange Server-Empfänger delegieren:

- Verwaltung aller Empfängereinstellungen
- Assistent für Exchange-Aufgaben verwenden
- Verwaltung von E-Mail-Adressen
- Konfigurieren allgemeiner Nachrichteneinstellungen
- Konfigurieren erweiterter Nachrichteneinstellungen

Dieser Container enthält außerdem Vorlagen, die den Zugriff auf einzelne, auf Exchange bezogene Eigenschaften von Benutzern, Gruppen und Kontakten steuern.

Um eine Zugriffsvorlage detailliert zu untersuchen, zeigen Sie das Dialogfeld **Eigenschaften** wie folgt an: Klicken Sie mit der rechten Maustaste auf Zugriffsvorlage und klicken Sie dann auf **Eigenschaften**. Auf der Registerkarte **Berechtigungen** im Dialogfeld **Eigenschaften** werden alle in der Zugriffsvorlage definierten Berechtigungseinträge aufgelistet. Sie können jeden Eintrag wie folgt untersuchen: Wählen Sie einen Eintrag aus, und klicken Sie auf die Schaltfläche **Anzeigen**.

Vordefinierte Zugriffsvorlagen von ActiveRoles Server können nicht geändert oder gelöscht werden. Wenn Sie Änderungen an einer vordefinierten Zugriffsvorlage vornehmen möchten, müssen Sie eine Kopie der Zugriffsvorlage erstellen und diese nach Bedarf verändern. Zum Erstellen einer Kopie klicken Sie mit der rechten Maustaste auf die Zugriffsvorlage und dann auf **Kopieren**.

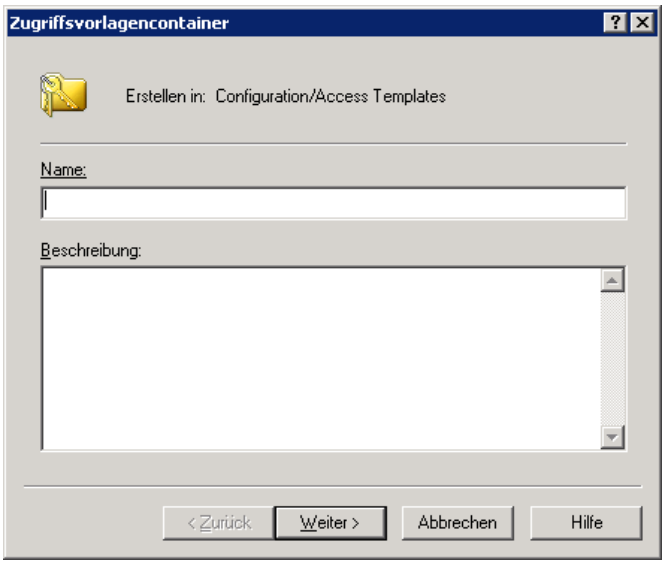
Sie können eine Zugriffsvorlage anwenden, indem Sie den Assistenten Delegation der Kontrolle verwenden: Klicken Sie mit der rechten Maustaste auf die Zugriffsvorlage, klicken Sie auf **Verknüpfungen**, und klicken Sie dann im Fenster **Verknüpfungen** auf **Hinzufügen**, um den Assistenten zu starten. Ausführlichere Informationen finden Sie unter „Anwenden von Zugriffsvorlagen" weiter unten in diesem Kapitel.

Erstellen einer Zugriffsvorlage

Die ActiveRoles Server-Konsole enthält den Assistenten Neues Objekt – Zugriffsvorlage zum Erstellen von Zugriffsvorlagen. Sie können den Assistenten auf folgende Weise starten: Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf **Access Templates**, und wählen Sie **Neu | Zugriffsvorlage** aus. In diesem Fall fügt der Assistent eine Zugriffsvorlage zum Container **Access Templates** hinzu.

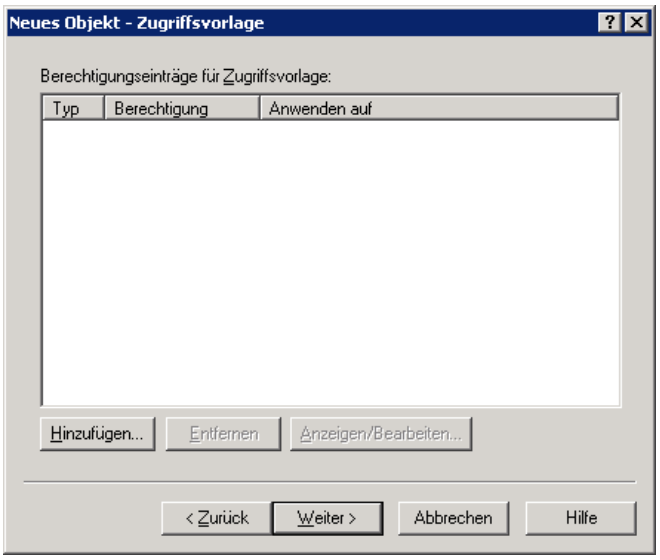
Sie sollten benutzerdefinierte Zugriffsvorlagen in einem separaten Container speichern. Sie können wie folgt einen Container erstellen: Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf **Access Templates**, und wählen Sie **Neu | Zugriffsvorlagencontainer** aus. Nachdem Sie einen Container erstellt haben, können Sie mit Hilfe des Assistenten eine Zugriffsvorlage zu dem Container anstatt direkt zu den **Access Templates** hinzufügen: Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf den Container, und wählen Sie **Neu | Zugriffsvorlage** aus.

Die erste Seite des Assistenten entspricht der folgenden Abbildung.



Geben Sie auf dieser Seite einen Namen und eine Beschreibung für die neue Zugriffsvorlage ein. Auf der ActiveRoles Server-Konsole werden im Bereich „Details" in der Liste der Zugriffsvorlagen der Name und die Beschreibung angezeigt.

Klicken Sie auf **Weiter**. Die zweite Seite des Assistenten ähnelt der folgenden Abbildung.

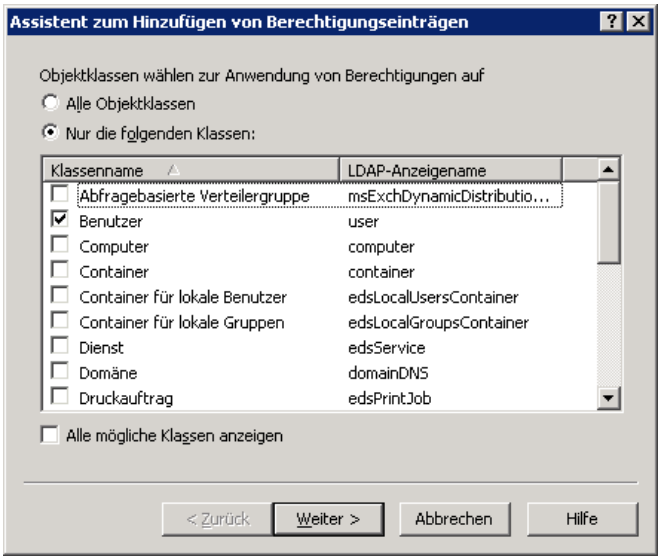


Auf dieser Seite werden Sie aufgefordert, eine Liste von Berechtigungseinträgen für Zugriffsvorlagen zu konfigurieren. Mit den Schaltflächen **Hinzufügen**, **Entfernen** und **Anzeigen/Bearbeiten** können Sie einen Eintrag hinzufügen, entfernen bzw. ändern. Durch Anklicken von **Hinzufügen** wird der Assistent zum Hinzufügen von Berechtigungseinträgen gestartet, der Sie bei der Konfiguration der Berechtigungseinträge unterstützt. Der Assistent wird weiter unten in diesem Abschnitt beschrieben.

Nachdem Sie die Liste der Berechtigungseinträge abgeschlossen haben, klicken Sie auf **Weiter** und dann auf **Fertig stellen**. Die neue Zugriffsvorlage wird erstellt.

Assistent zum Hinzufügen von Berechtigungseinträgen

Der Assistent zum Hinzufügen von Berechtigungseinträgen ermöglicht Ihnen die Festlegung der Berechtigungen, die zur Zugriffsvorlage hinzugefügt werden sollen. Die erste Seite des Assistenten entspricht der folgenden Abbildung.

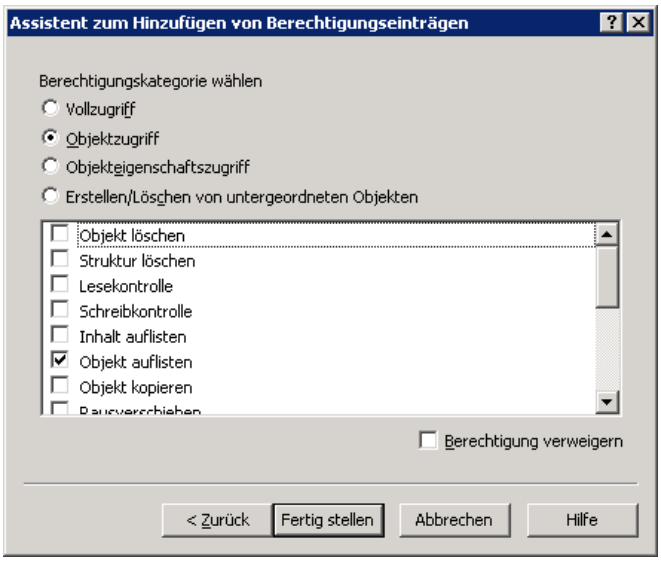


Auf dieser Seite wählen Sie die Typen von Objekten aus, denen Sie mit dieser Berechtigung den Zugriff gewähren (oder verweigern) möchten. Sie können eine der folgenden Optionen auswählen:

- **Alle Objektklassen** Mit dieser Option steuert die Berechtigung den Zugriff auf Objekte beliebigen Typs.
- **Nur die folgenden Klassen** Mit dieser Option steuert die Berechtigung den Zugriff auf Objekte des Typs, den Sie auswählen, indem Sie die entsprechenden Kontrollkästchen in der Liste aktivieren.

Standardmäßig werden nicht alle Objektklassen in der Liste angezeigt. Um alle Objektklassen anzuzeigen, aktivieren Sie das Kontrollkästchen **Alle möglichen Klassen anzeigen**.

Klicken Sie nach dem Auswählen der gewünschten Objektklassen auf **Weiter**. Die nächste Seite des Assistenten entspricht der folgenden Abbildung.



Auf dieser Seite wählen Sie eine Berechtigungskategorie aus und geben an, ob die Berechtigung bestimmte administrative Aktionen zulassen oder verweigern soll.

Sie können eine der folgenden Berechtigungskategorien auswählen:

- **Vollzugriff** Lässt alle administrativen Aktionen für ein Objekt zu oder verweigert sie.
- **Objektzugriff** Steuert, wie auf ein Objekt zugegriffen und wie es kontrolliert wird.
- **Objekteigenschaftszugriff** Steuert den Zugriff auf die Attribute eines Objekts.
- **Erstellen/Löschen von untergeordneten Objekten** Gewährt oder verweigert die Erstellung oder Löschung von Objekten in einem Container.

Wenn die Berechtigung bestimmte administrative Aktionen verweigern soll, aktivieren Sie das Kontrollkästchen **Berechtigung verweigern**.

In den folgenden Abschnitten werden die Berechtigungskategorien erörtert, die Sie im Assistenten Berechtigungseinträge hinzufügen auswählen können.

Vollzugriff

Die Berechtigungen in dieser Kategorie decken alle administrativen Vorgänge für Objekte (und ihre Eigenschaften) der Klassen ab, die Sie im vorigen Schritt des Assistenten Berechtigungseinträge hinzufügen ausgewählt haben.

Wählen Sie **Vollzugriff** aus, und klicken Sie auf **Fertig stellen**, um die Berechtigung der neu erstellten Zugriffsvorlage hinzuzufügen.

Objektzugriff

Die Berechtigungen in dieser Kategorie decken alle administrativen Vorgänge für Objekte (jedoch nicht ihre Eigenschaften) der Klassen ab, die Sie im vorigen Schritt des Assistenten Berechtigungseinträge hinzufügen ausgewählt haben.

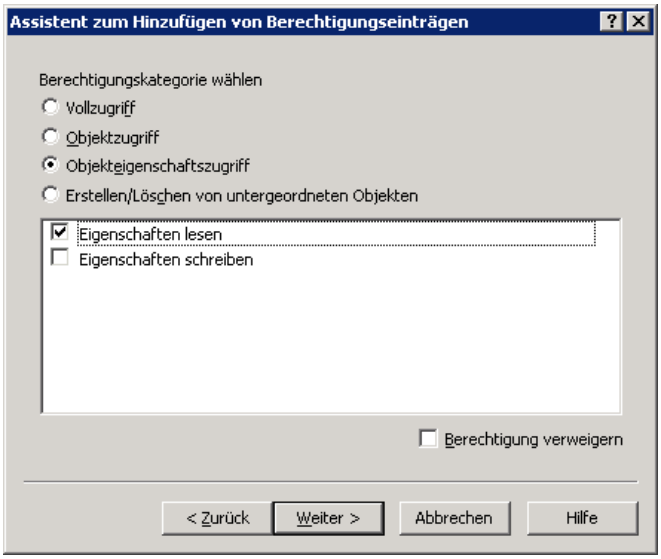
Administrative Vorgänge werden in der Liste ausgewählt, die bei Auswahl von **Objektzugriff** angezeigt wird. Sie wählen die notwendigen Vorgänge aus, indem Sie die entsprechenden Kontrollkästchen aktivieren. Beispielsweise können Sie **Objekt auflisten** auswählen, um das Anzeigen von Objekten bestimmter Typen zuzulassen.

Nachdem Sie die Vorgänge ausgewählt haben, klicken Sie auf **Fertig stellen**, um den Assistent Berechtigungseinträge hinzufügen abzuschließen. Die Berechtigung wird der neu erstellten Zugriffsvorlage hinzugefügt.

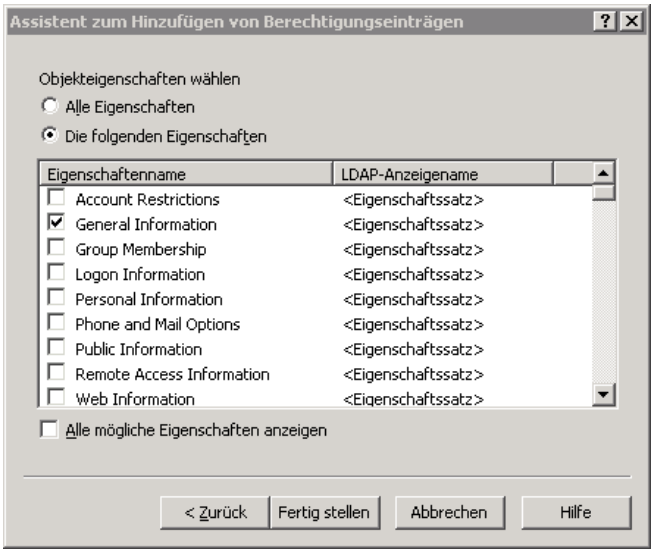
Objekteigenschaftszugriff

Die Berechtigungen in dieser Kategorie decken administrativen Vorgänge für Objekteigenschaften für Objekte der Klassen ab, die Sie im vorigen Schritt des Assistenten Berechtigungseinträge hinzufügen ausgewählt haben.

Wenn Sie **Objekteigenschaftszugriff** auswählen, geben Sie den Zugriff auf Objekteigenschaften an. Sie können **Eigenschaften lesen** und **Eigenschaften schreiben** auswählen, wie in der folgenden Abbildung gezeigt.



Nach dem Klicken auf **Weiter** zeigt der Assistent eine Seite an, auf der Sie die Eigenschaften auswählen können, für die die Berechtigung den Zugriff zulassen (oder verweigern) soll. Die Seite entspricht der folgenden Abbildung:



Auf dieser Seite können Sie eine der folgenden Optionen auswählen:

- **Alle Eigenschaften** Mit dieser Option steuert die Berechtigung den Zugriff auf alle Eigenschaften.
- **Die folgenden Eigenschaften** Mit dieser Option steuert die Berechtigung den Zugriff auf die Eigenschaften, die Sie in der Liste auswählen, indem Sie die entsprechenden Kontrollkästchen aktivieren.

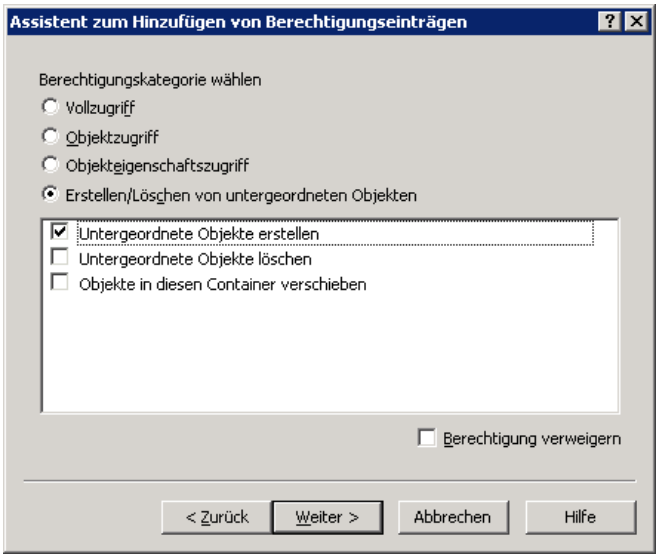
Standardmäßig werden nicht alle Objekteigenschaften in der Liste angezeigt. Um alle Objekteigenschaften anzuzeigen, aktivieren Sie das Kontrollkästchen **Alle möglichen Eigenschaften anzeigen**.

Nachdem Sie die gewünschten Eigenschaften ausgewählt haben, klicken Sie auf **Fertig stellen**, um den Assistent Berechtigungseinträge hinzufügen abzuschließen. Die Berechtigung wird der Zugriffsvorlage hinzugefügt.

Erstellen/Löschen von Berechtigungen für untergeordnete Objekte

Die Berechtigungen in dieser Kategorie decken die Erstellung und Löschung untergeordneter Objekte in Containerobjekten der Klassen ab, die Sie im vorigen Schritt des Assistenten Berechtigungseinträge hinzufügen ausgewählt haben.

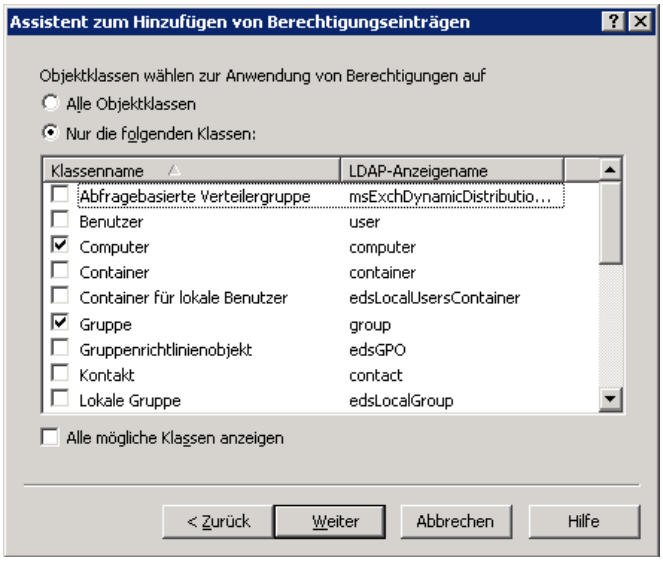
Durch Auswählen von **Erstellen/Löschen von untergeordneten Objekten** geben Sie die Erstellungs-, Lösch- und Verschiebungsvorgänge an, die die Berechtigung zulassen (oder verweigern) soll. Die Liste der Vorgänge wird in der folgenden Abbildung gezeigt.



Sie können folgende Vorgänge wählen:

- **Untergeordnete Objekte erstellen** Steuert die Erstellung untergeordneter Objekte der Klassen, die Sie im nächsten Schritt auswählen.
- **Untergeordnete Objekte löschen** Steuert die Löschung untergeordneter Objekte der Klassen, die Sie im nächsten Schritt auswählen.
- **Objekte in diesen Container verschieben** Steuert die Verschiebung von Objekten der Klassen, die Sie im nächsten Schritt auswählen. Für diesen Vorgang wird angenommen, dass Objekte ohne die Berechtigung zum Löschen vorhandener Objekte oder zum Erstellen neuer Objekte von einem Container in einen anderen verschoben werden.

Nach dem Klicken auf **Weiter** zeigt der Assistent die Seite an, auf der Sie die Typen von Objekten auswählen können, für die die Berechtigung die im vorigen Schritt ausgewählten Vorgänge zulassen (oder verweigern) soll. Die Seite entspricht der folgenden Abbildung:



Auf dieser Seite wählen Sie die Typen von Objekten aus, für die Sie mit dieser Berechtigung den Erstellungs-, Lösch- oder Verschiebungsvorgang zulassen (oder verweigern) möchten. Sie können eine der folgenden Optionen auswählen:

- **Alle Objektklassen** Mit dieser Option steuert die Berechtigung die Vorgänge für Objekte beliebigen Typs.
- **Nur die folgenden Klassen** Mit dieser Option steuert die Berechtigung die Vorgänge an Objekten des Typs, den Sie in der Liste auswählen, indem Sie die entsprechenden Kontrollkästchen aktivieren.

Standardmäßig werden nicht alle Objektklassen in der Liste angezeigt. Um alle Objektklassen anzuzeigen, aktivieren Sie das Kontrollkästchen **Alle möglichen Klassen anzeigen**.

Nachdem Sie die Objektklassen ausgewählt haben, klicken Sie auf **Fertig stellen**, um den Assistent Berechtigungseinträge hinzufügen abzuschließen. Die Berechtigung wird der Zugriffsvorlage hinzugefügt.

Schrittweise Anleitungen bezüglich der Erstellung einer Zugriffsvorlage finden Sie unter **Anleitungen/Verwalten von Zugriffsvorlagen/Erstellen von Zugriffsvorlagen** in der ActiveRoles Server-Hilfe.

Anwenden von Zugriffsvorlagen

Mit ActiveRoles Server können Zugriffsvorlagen auf beliebige Objekte angewendet werden: administrative Ansichten (verwaltete Einheiten), Verzeichnisordner (Container) oder einzelne Objekte (Blattobjekte).

Beim Anwenden einer Zugriffsvorlage auf ein Objekt wählen Sie einen Trustee (Benutzer oder Gruppe) aus und weisen dem Trustee für dieses Objekt Berechtigungen zu. Folglich erhält der Trustee Zugriff auf das Objekt gemäß den in der Zugriffsvorlage definierten Berechtigungen.

So kann beispielsweise zwei Assistenten eines Verzeichnisadministrators ein Vollzugriff auf verschiedene Domänen gewährt werden. Dem Help Desk kann eine Administratorfunktion zum Zurücksetzen von Kennwörtern zugewiesen werden.

Wenn Sie Zugriffsvorlagen auf einen Ordner anwenden, können Sie die Berechtigungseinstellungen so konfigurieren, dass sie von dem Ordner an seine untergeordneten Objekte weiter unten in der Verzeichnisstruktur weitergegeben werden.

Zum Anwenden einer Zugriffsvorlage müssen Sie den Assistenten zum Delegieren der Kontrolle starten und abschließen.

Sie können den Assistenten zum Delegieren der Kontrolle von jeder der nachfolgend aufgeführten Positionen starten:

- **Zugriffsvorlage** Klicken Sie mit der rechten Maustaste auf Zugriffsvorlage, klicken Sie dann auf **Verknüpfungen** und klicken Sie anschließend auf die Schaltfläche **Hinzufügen**. Zugriffsvorlagen befinden sich im Container **Configuration/Access Templates**.

  Wenn der Assistent auf diese Weise gestartet wird, können Sie Verzeichnisobjekte auswählen, in denen die Zugriffsvorlage und die Trustees für diese Objekte angewendet werden sollen.

- **Sicherbares Objekt** Abhängig davon, ob das Objekt ein Container- oder ein Blattobjekt ist, führen Sie eine der folgenden Aktionen aus:

  - Wenn es sich um einen Container oder eine verwaltete Einheit handelt, klicken Sie mit der rechten Maustaste darauf, klicken Sie auf **Kontrolle delegieren**, und klicken Sie dann auf die Schaltfläche **Hinzufügen**.
  - Wenn es sich um ein Blattobjekt handelt, zeigen Sie das Dialogfeld **Eigenschaften** an, wechseln Sie zur Registerkarte **Verwaltung**, klicken Sie auf die Schaltfläche **Sicherheit** und dann auf die Schaltfläche **Hinzufügen**.

  Wenn der Assistent auf diese Weise gestartet wird, können Sie Trustees für das Objekt sowie Zugriffsvorlagen auswählen, in denen die Rechte der Trustees für das Objekt definiert werden sollen.

- **Sicherheitsprinzipal (Trustee)** Klicken Sie mit der rechten Maustaste auf die Gruppe oder den Benutzer, die bzw. den Sie als Trustee auswählen möchten, klicken Sie auf **Delegierte Rechte**, und klicken Sie dann auf die Schaltfläche Hinzufügen.

  Wenn der Assistent auf diese Weise gestartet wird, können Sie Objekte auswählen, für die Sie den Trustee und die Zugriffsvorlagen auswählen möchten, in denen die Rechte der Trustees für diese Objekte definiert werden sollen.

Sie können den Assistenten Delegation der Kontrolle auch vom erweiterten Bereich „Details" aus starten (stellen Sie sicher, dass **Erweiterte Detailansicht** im Menü **Ansicht** aktiviert ist):

- Wählen Sie eine Zugriffsvorlage aus, klicken Sie mit der rechten Maustaste in einen leeren Bereich auf der Registerkarte **Verknüpfungen**, und klicken Sie dann auf **Hinzufügen**.

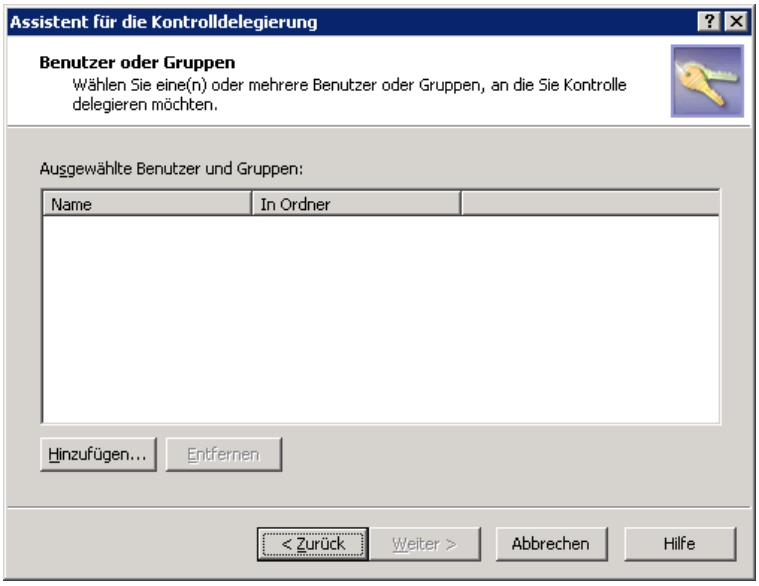
  Wenn der Assistent auf diese Weise gestartet wird, können Sie Verzeichnisobjekte auswählen, in denen die Zugriffsvorlage und die Trustees für diese Objekte angewendet werden sollen.

- Wählen Sie ein Verzeichnisobjekt (sicherbares Objekt) aus, klicken Sie mit der rechten Maustaste in einen leeren Bereich auf der Registerkarte **AR-Serversicherheit**, und klicken Sie dann auf **Hinzufügen**.

  Wenn der Assistent auf diese Weise gestartet wird, können Sie Trustees für das Objekt sowie Zugriffsvorlagen auswählen, in denen die Rechte der Trustees für das Objekt definiert werden sollen.

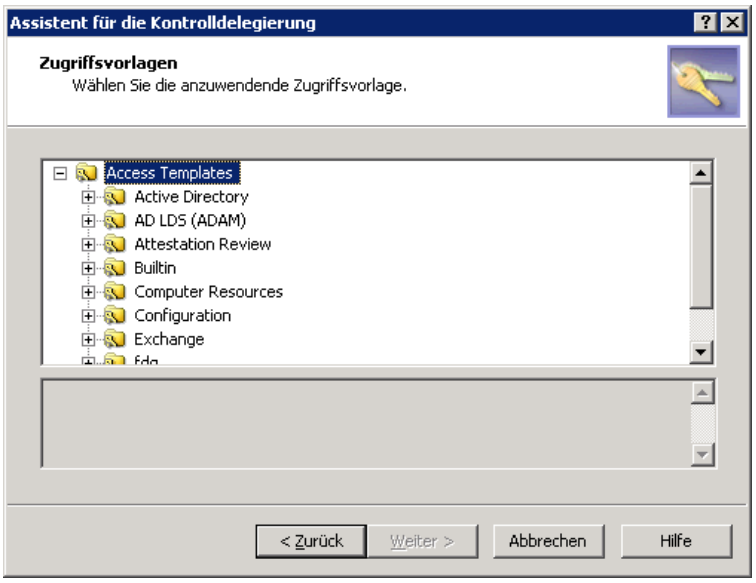
Der Rest dieses Abschnitts enthält Anweisungen zum Abschließen des Assistenten Delegation der Kontrolle. Dabei wird angenommen, dass Sie den Assistenten von dem Objekt aus starten, für das Sie die Kontrolle delegieren möchten (von einem sicherbaren Objekt). Anleitungen, wie Sie den Assistenten in anderen Fällen abschließen, finden Sie unter **Anleitungen/Verwalten von Zugriffsvorlagen/Anwenden von Zugriffsvorlagen** in der ActiveRoles Server-Hilfe.

Wenn Sie den Assistenten für die Kontrolldelegierung von einem sicherbaren Objekt aus starten, können Sie auf der Seite **Willkommen** auf **Weiter** klicken, um die Seite **Benutzer oder Gruppen** anzuzeigen. Diese wird in der folgenden Abbildung gezeigt.



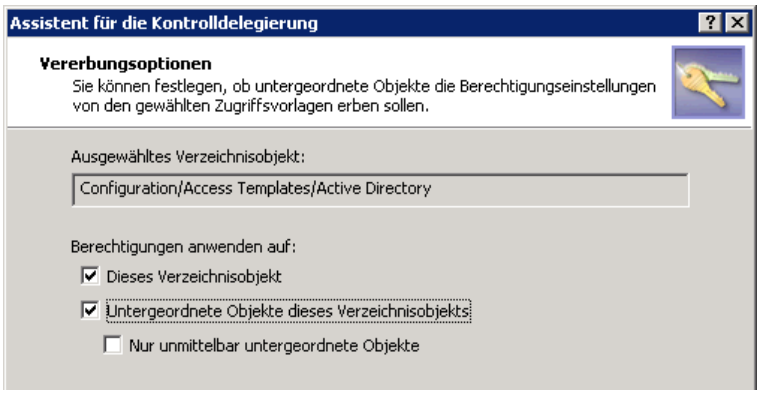
Klicken Sie auf der Seite **Benutzer oder Gruppen** auf **Hinzufügen**, um das Dialogfeld **Objekte auswählen** anzuzeigen, in dem Sie Gruppen oder Benutzer auswählen können, die zu Trustees ernannt werden sollen. Geben Sie die Namen der Benutzer oder Gruppen, die Sie zur Liste hinzufügen möchten, ein oder wählen Sie diese aus und klicken Sie dann auf **OK**.

Klicken Sie nach dem Abschließen der Liste auf der Seite **Benutzer oder Gruppen** auf **Weiter**. Nun wird die Seite **Zugriffsvorlagen** angezeigt, die in der folgenden Abbildung gezeigt wird.



Erweitern Sie auf der Seite **Zugriffsvorlagen** Container, die Zugriffsvorlagen enthalten, und aktivieren Sie Kontrollkästchen neben den Namen der Zugriffsvorlagen, die Sie anwenden möchten.

Klicken Sie nach dem Auswählen aller gewünschten Zugriffsvorlagen auf **Weiter**. Nun wird die Seite **Vererbungsoptionen** angezeigt, die in der folgenden Abbildung gezeigt wird.

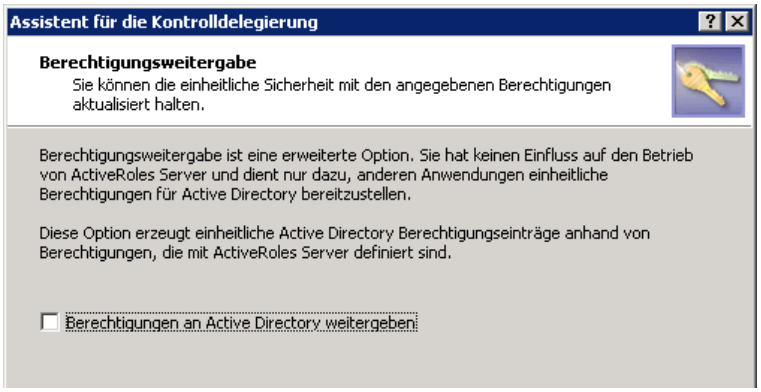

Assistent für die Kontrolldelegierung
Vererbungsoptionen
Sie können festlegen, ob untergeordnete Objekte die Berechtigungseinstellungen von den gewählten Zugriffsvorlagen erben sollen.
Ausgewähltes Verzeichnisobjekt:
Configuration/Access Templates/Active Directory
Berechtigungen anwenden auf:
Dieses Verzeichnisobjekt
Untergeordnete Objekte dieses Verzeichnisobjekts
Nur unmittelbar untergeordnete Objekte

Auf der Seite **Vererbungsoptionen** können Sie die folgenden Optionen auswählen, um die Vererbung von Berechtigungen zu kontrollieren:

- **Dieses Verzeichnisobjekt** Stellt sicher, dass die Trustees über Administratorrechte für das sicherbare Objekt selbst verfügen.
- **Untergeordnete Objekte dieses Verzeichnisobjekts** Stellt sicher, dass die Trustees über Administratorrechte für die untergeordneten Objekte des sicherbaren Objekts verfügen, die in der Verzeichnisstruktur unter ihm liegen.
- **Nur unmittelbar untergeordnete Objekte** Beschränkt die Rechte der Trustees auf die unmittelbar untergeordneten Objekte des sicherbaren Objekts.

Standardmäßig sind die ersten beiden Optionen ausgewählt.

Klicken Sie auf **Weiter**. Nun wird die Seite **Berechtigungsweitergabe** angezeigt, die in der folgenden Abbildung gezeigt wird.


Assistent für die Kontrolldelegierung
Berechtigungsweitergabe
Sie können die einheitliche Sicherheit mit den angegebenen Berechtigungen aktualisiert halten.
Berechtigungsweitergabe ist eine erweiterte Option. Sie hat keinen Einfluss auf den Betrieb von ActiveRoles Server und dient nur dazu, anderen Anwendungen einheitliche Berechtigungen für Active Directory bereitzustellen.
Diese Option erzeugt einheitliche Active Directory Berechtigungseinträge anhand von Berechtigungen, die mit ActiveRoles Server definiert sind.
Berechtigungen an Active Directory weitergeben

Auf der Seite **Berechtigungsverbreitung** können Sie das Kontrollkästchen **Berechtigungen an Active Directory weitergeben** aktivieren. Wenn Sie es aktivieren, werden die Berechtigungseinstellungen, die Sie konfigurieren, nach Active Directory synchronisiert. Dies führt dazu, dass die Trustees ihre Rechte auch außerhalb der ActiveRoles Server-Umgebung wahrnehmen können. Dadurch entsteht das Risiko, dass sie mit ActiveRoles Server konfigurierte und durchgesetzte Richtlinien umgehen könnten. Daher sollten Sie diese Option wohl überlegt verwenden.

Standardmäßig ist das Kontrollkästchen **Berechtigungen an Active Directory weitergeben** deaktiviert. Wenn Sie sich entschließen, diese Option zu verwenden, können Sie diese Einstellung jederzeit ändern, indem Sie die Schaltfläche **Mit AD synchronisieren** im Fenster **ActiveRoles Server-Sicherheit** oder den Befehl **Mit AD synchronisieren** in der erweiterten Detailanzeige verwenden (siehe „Synchronisieren von Berechtigungen nach Active Directory" weiter unten in diesem Kapitel).

Klicken Sie auf **Weiter**, und klicken Sie dann auf **Fertig stellen**, um den Assistenten abzuschließen.

Verwalten von Zugriffsvorlagenverknüpfungen

Beim Anwenden einer Zugriffsvorlage erstellt ActiveRoles Server eine Zugriffsvorlagenverknüpfung. Administratorrechte werden also durch Verknüpfen von Zugriffsvorlagen mit sicherbaren Objekten angegeben, d.h. mit verwalteten Einheiten, Verzeichnisordnern (Containern) oder einzelnen Objekten (Blattobjekten).

Jede Zugriffsvorlagenverknüpfung umfasst den Bezeichner (Security ID, SID) des Sicherheitsprinzipals (des Benutzers oder der Gruppe), dem die angegebenen Administratorrechte zugewiesen sind. Bei der Erstellung einer Zugriffsvorlagenverknüpfung wird der Benutzer oder die Gruppe zum Trustee für die Objektauflistung oder den Ordner, mit dem die Zugriffsvorlage verknüpft ist. Die Berechtigungen werden dabei durch diese Zugriffsvorlage angegeben.

Wenn eine Zugriffsvorlage geändert oder nicht mehr angewendet wird, werden die Berechtigungsinformationen für Objekte, auf die sich die Zugriffsvorlage auswirkt, entsprechend geändert.

Sie können über eine der folgenden Möglichkeiten eine Liste von Zugriffsvorlagenverknüpfungen anzeigen:

- **Zugriffsvorlage** Klicken Sie mit der rechten Maustaste auf eine Zugriffsvorlage und klicken Sie dann auf **Verknüpfungen**.

  Dies zeigt die Verknüpfungen an, in denen die Zugriffsvorlage auftritt.

- **Sicherheitsprinzipal (Trustee)** Klicken Sie mit der rechten Maustaste auf eine Gruppe oder einen Benutzer, und klicken Sie dann auf **Delegierte Rechte**.

  Dann werden die Verknüpfungen angezeigt, in denen die Gruppe oder der Benutzer direkt oder aufgrund von Gruppenmitgliedschaften als Trustee auftritt.

- **Sicherbares Objekt** Klicken Sie mit der rechten Maustaste auf ein Containerobjekt oder eine verwaltete Einheit und klicken Sie dann auf **Kontrolle delegieren**. Für ein Blattobjekt öffnen Sie das Dialogfeld **Eigenschaften**, öffnen die Registerkarte **Verwaltung** und klicken auf **Sicherheit**.

  Dann werden die Verknüpfungen angezeigt, in denen das ausgewählte Objekt als sicherbares Objekt (bezeichnet als *Verzeichnisobjekt*) auftritt.

Sie können eine Liste von Zugriffsvorlagenverknüpfungen auch im erweiterten Bereich „Details" anzeigen. Stellen Sie sicher, dass im Menü **Ansicht** die Option **Erweiterte Detailansicht** aktiviert ist, und wählen Sie dann eine der folgenden Möglichkeiten aus:

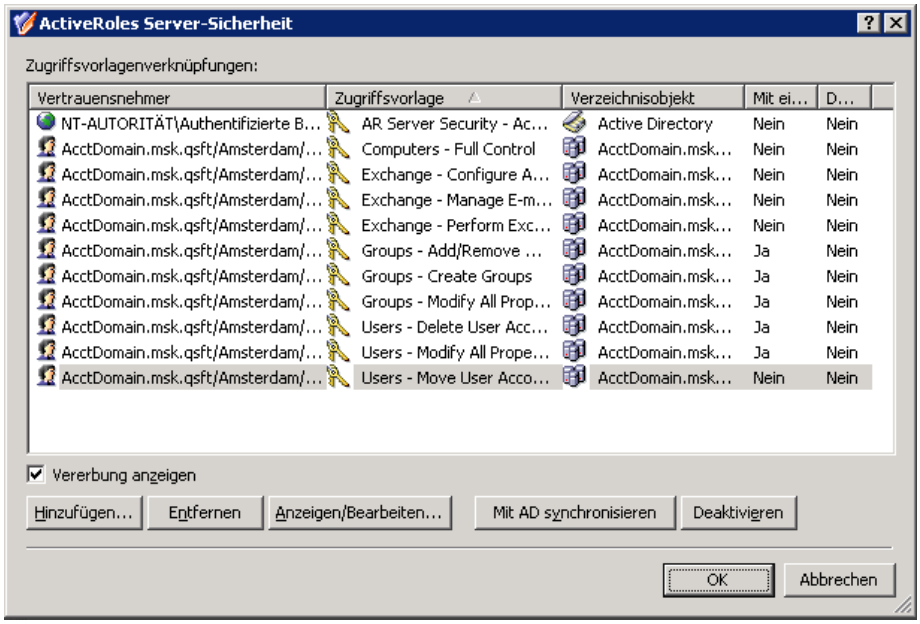
- Zugriffsvorlage

  Auf der Registerkarte **Verknüpfungen** werden die Verknüpfungen aufgelistet, in denen die ausgewählte Zugriffsvorlage auftritt.

- Anderes Objekt (verwaltete Einheit, Container oder Blattobjekt)

  Auf der Registerkarte **AR-Serversicherheit** werden die Verknüpfungen aufgelistet, in denen das ausgewählte Objekt als sicherbares Objekt (bezeichnet als Verzeichnisobjekt) auftritt.

Die ActiveRoles Server-Konsole zeigt eine Liste der Zugriffsvorlagenverknüpfungen in einem separaten Fenster an. Daher wird das Fenster **ActiveRoles Server-Sicherheit** angezeigt, wenn Sie von einem sicherbaren Objekt aus starten (zum Beispiel durch Anklicken einer verwalteten Einheit oder Organisationseinheit und anschließendes Anklicken von **Kontrolle delegieren**):


ActiveRoles Server-Sicherheit
Zugriffsvorlagenverknüpfungen:
Vertrauensnehmer
Zugriffsvorlage
Verzeichnisobjekt
Mit ei...
D...
NT-AUTORITÄT\Authentifizierte B... AR Server Security - Ac... Active Directory Nein Nein
AcctDomain.msk.qsft/Amsterdam/... Computers - Full Control AcctDomain.msk... Nein Nein
AcctDomain.msk.qsft/Amsterdam/... Exchange - Configure A... AcctDomain.msk... Nein Nein
AcctDomain.msk.qsft/Amsterdam/... Exchange - Manage E-m... AcctDomain.msk... Nein Nein
AcctDomain.msk.qsft/Amsterdam/... Exchange - Perform Exc... AcctDomain.msk... Nein Nein
AcctDomain.msk.qsft/Amsterdam/... Groups - Add/Remove ... AcctDomain.msk... Ja Nein
AcctDomain.msk.qsft/Amsterdam/... Groups - Create Groups AcctDomain.msk... Ja Nein
AcctDomain.msk.qsft/Amsterdam/... Groups - Modify All Prop... AcctDomain.msk... Ja Nein
AcctDomain.msk.qsft/Amsterdam/... Users - Delete User Acc... AcctDomain.msk... Ja Nein
AcctDomain.msk.qsft/Amsterdam/... Users - Modify All Prope... AcctDomain.msk... Ja Nein
AcctDomain.msk.qsft/Amsterdam/... Users - Move User Acco... AcctDomain.msk... Nein Nein
Vererbung anzeigen
Hinzufügen...
Entfernen
Anzeigen/Bearbeiten...
Mit AD synchronisieren
Deaktivieren
OK
Abbrechen

Jeder Eintrag in der Liste der Zugriffsvorlagenverknüpfungen schließt die folgenden Informationen ein:

- **Vertrauensnehmer** Die Verknüpfung definiert Administratorrechte dieses Sicherheitsprinzipals (Gruppe oder Benutzer).
- **Zugriffsvorlage** Die Zugriffsvorlage, die die Rechte des Trustees bestimmt.
- **Verzeichnisobjekt** Die Verknüpfung definiert die Rechte des Trustees für dieses sicherbare Objekt.
- **Mit einheitlicher Sicherheit synchronisieren** Gibt an, ob ActiveRoles Server Berechtigungen nach Active Directory synchronisiert.
- **Deaktiviert** Gibt an, ob die Berechtigungen tatsächlich angewendet werden. Wenn eine Verknüpfung deaktiviert ist, kann der Trustee die Administratorrechte nicht ausüben, die durch sie definiert werden.

Im Fenster **ActiveRoles Server-Sicherheit** (sowie auch im erweiterten Detailfenster auf der Registerkarte **AR-Serversicherheit**) werden die Verknüpfungen der folgenden Kategorien aufgelistet:

- **Direkte Verknüpfungen** Die Zugriffsvorlage wird direkt auf das ausgewählte sicherbare Objekt angewendet (mit ihm verknüpft).
- **Geerbte Verknüpfungen** Die Zugriffsvorlage wird auf einen Container in der Containerhierarchie über dem ausgewählten sicherbaren Objekt oder auf eine verwaltete Einheit, zu der das sicherbare Objekt gehört, angewendet (mit ihm/ihr verknüpft).

Die von übergeordneten Objekte geerbten Verknüpfungen können aus der Liste herausgefiltert werden:

- Deaktivieren Sie bei Verwendung des Fensters **ActiveRoles Server-Sicherheit** das Kontrollkästchen **Vererbung anzeigen**.
- Bei Verwendung der Registerkarte **AR-Serversicherheit** klicken Sie mit der rechten Maustaste auf die Liste und klicken dann auf **Vererbung anzeigen**, um das Menüelement zu deaktivieren.

In einem Fenster oder auf einer Registerkarte, wo Zugriffsvorlagenverknüpfungen angezeigt werden, können Sie Verknüpfungen verwalten. In einem Fenster können Sie die Schaltflächen unter der Liste verwenden. Auf einer Registerkarte können Sie mit der rechten Maustaste auf einen Listeneintrag oder in einen leeren Bereich klicken und dann Befehle im Kontextmenü verwenden. So werden zum Beispiel die folgenden Schaltflächen im Fenster **ActiveRoles Server-Sicherheit** angezeigt:

- **Hinzufügen** Startet den Assistenten Delegation der Kontrolle für die Erstellung/Anwendung von Zugriffsvorlagen.
- **Entfernen** Löscht die ausgewählten Einträge aus der Verknüpfungsliste. Nur für direkte Verknüpfungen verfügbar.
- **Anzeigen/Bearbeiten** Zeigt das Dialogfeld an, in dem Verknüpfungseigenschaften angezeigt oder geändert werden können, z.B. Optionen für die Vererbung und die Weitergabe von Berechtigungen.
- **Mit AD synchronisieren** Schaltet die Option für die Berechtigungsweitergabe für die in der Liste ausgewählten Verknüpfungen um.
- **Deaktivieren** Deaktiviert oder aktiviert die Verknüpfung. Wenn eine Verknüpfung deaktiviert ist, haben die von ihr angegebenen Berechtigungen keine Auswirkungen.

Im Fenster **ActiveRoles Server-Sicherheit** ist die Schaltfläche **Entfernen** nur für direkte Verknüpfungen verfügbar. Wenn Sie Verknüpfungen löschen möchten, sollten Sie sie mit dem Befehl **Verknüpfungen** für die Zugriffsvorlage verwalten.

Schrittweise Anleitungen bezüglich der Anwendung einer Zugriffsvorlage und der Änderung von Zugriffsvorlagenverknüpfungen finden Sie unter **Anleitungen/Verwalten von Zugriffsvorlagen/Anwenden einer Zugriffsvorlage** und **Anleitungen/Verwalten von Zugriffsvorlagen/Verwalten von Zugriffsvorlagenverknüpfungen** in der ActiveRoles Server-Hilfe.

Synchronisieren von Berechtigungen nach Active Directory

ActiveRoles Server stellt die Option bereit, die einheitliche Sicherheit von Active Directory anhand ausgewählter Berechtigungen aktuell zu halten, die mit Hilfe von Zugriffsvorlagen angegeben werden. Diese Option, die als *„Weitergabe von Berechtigungen*" bezeichnet wird, soll Benutzern und Anwendungen einheitliche Berechtigungen für Active Directory bereitstellen. Im normalen Betrieb von ActiveRoles Server wird diese Option nicht verwendet.

Sie können die Option für die Weitergabe von Berechtigungen auf folgende Weisen festlegen:

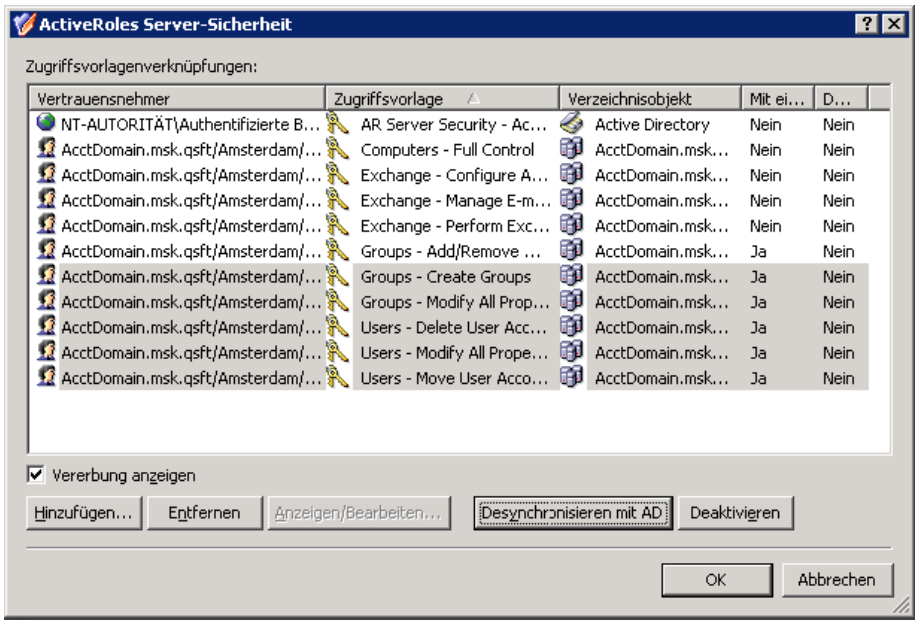
- Beim Anwenden von Zugriffsvorlagen können Sie das Kontrollkästchen **Berechtigungen an Active Directory weitergeben** im Assistenten Delegation der Kontrolle auswählen.
- Beim Verwalten von Zugriffsvorlagenverknüpfungen können Sie die Schaltfläche **Mit AD synchronisieren** in einem Fenster verwenden, in dem eine Liste von Verknüpfungen angezeigt wird, oder den Befehl **Mit AD synchronisieren** auf einer Registerkarte, auf der im erweiterten Detailfenster eine Liste von Verknüpfungen angezeigt wird, ausführen.

Nehmen Sie beispielsweise an, dass ActiveRoles Server bestimmte Berechtigungen für eine Organisationseinheit definiert und dass Sie sie nach Active Directory synchronisieren möchten. Sie können diese Aufgabe wie folgt ausführen.

Klicken Sie zunächst mit der rechten Maustaste auf die Organisationseinheit, und klicken Sie auf **Kontrolle delegieren**, um das Fenster **ActiveRoles Server-Sicherheit** anzuzeigen.

Wählen Sie dann in der Liste **Zugriffsvorlagenverknüpfungen** die Verknüpfungen aus, die die zu synchronisierenden Berechtigungen definieren.

Klicken Sie zum Schluss auf die Schaltfläche **Mit AD synchronisieren**. Die Spalte **Mit nativer Sicherheit synchronisieren** in der Liste zeigt **Ja** für die Verknüpfungen an, die Sie synchronisieren werden (siehe folgende Abbildung).



Nachdem Sie auf **OK** geklickt haben, erstellt ActiveRoles Server Berechtigungen in Active Directory, sodass der Trustee anhand der Zugriffsvorlagenverknüpfungen, die Sie synchronisiert haben, in Active Directory über die gleichen Rechte verfügt wie in der ActiveRoles Server-Umgebung.

Sie können die Synchronisierung von Berechtigungen jederzeit beenden, indem Sie auf die Schaltfläche **Desynchronisieren mit AD** klicken. Dann löscht ActiveRoles Server alle Berechtigungseinträge in Active Directory, die durch die Synchronisierung erstellt wurden.

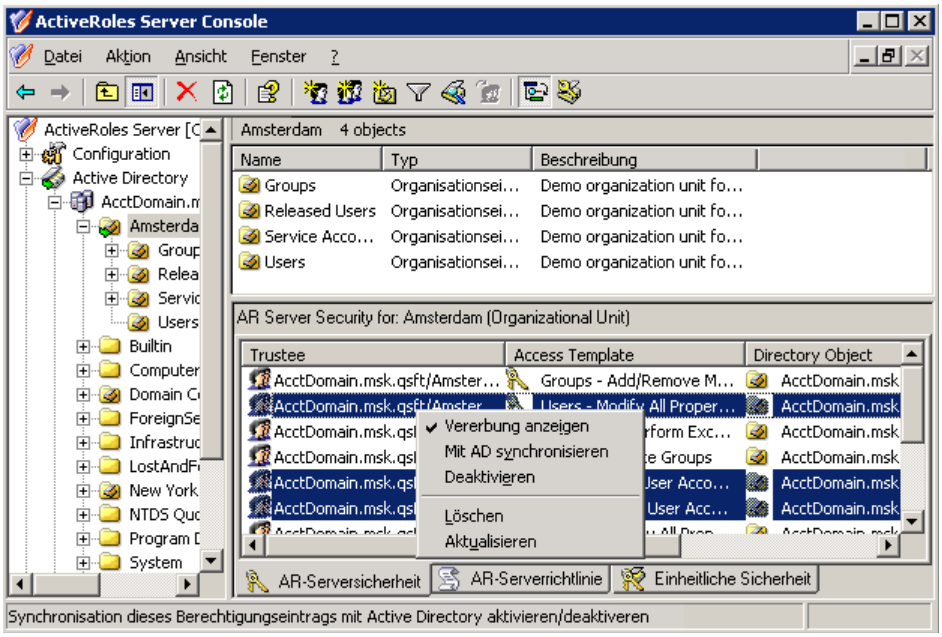
Im Fenster **ActiveRoles Server-Sicherheit** ist die Schaltfläche **Mit AD synchronisieren** nur für direkte Verknüpfungen verfügbar. Wenn Sie Verknüpfungen synchronisieren möchten, sollten Sie sie mit dem Befehl **Verknüpfungen** für die Zugriffsvorlage verwalten.

Sie können diese Aufgabe auch wie folgt im erweiterten Detailfenster ausführen.

Wählen Sie zuerst die Organisationseinheit aus.

Wählen Sie dann auf der Registerkarte **AR-Serversicherheit** die Zugriffsvorlagenverknüpfungen aus, die die zu synchronisierenden Berechtigungen definieren.

Klicken Sie zum Schluss mit der rechten Maustaste auf die Auswahl, und klicken Sie dann auf **Mit AD synchronisieren**, wie in der folgenden Abbildung gezeigt.



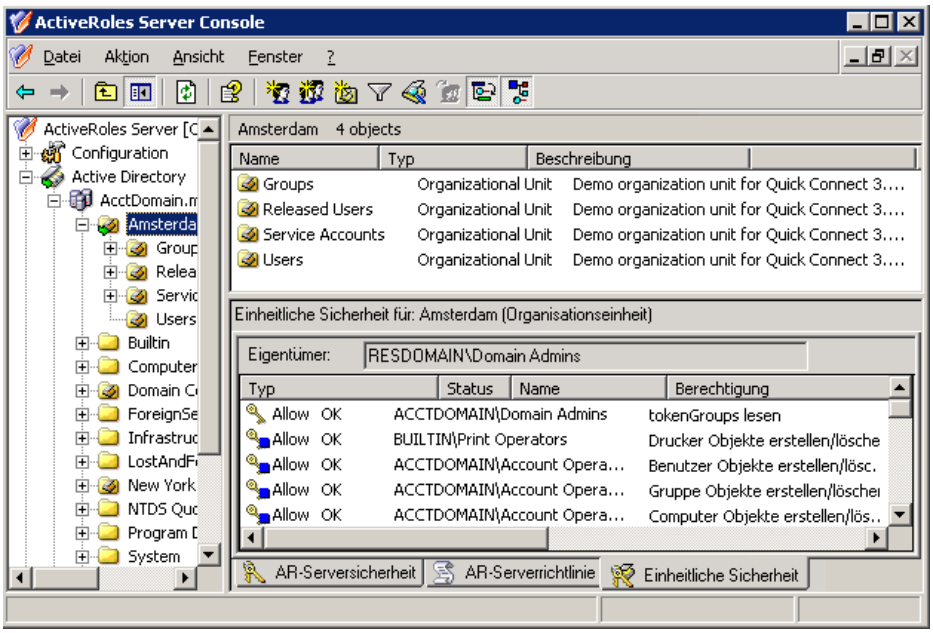
Sie können den Befehl **Mit AD synchronisieren** benutzen, um die Synchronisation zu stoppen: Klicken Sie mit der rechten Maustaste auf die Verknüpfungen, die nicht mehr synchronisiert werden sollen, und klicken Sie dann auf **Desynchronisieren mit AD**.

Auf der Registerkarte **AR Server-Sicherheit** ist der Befehl **Mit AD synchronisieren** nur für direkte Verknüpfungen verfügbar. Wenn Sie Verknüpfungen synchronisieren möchten, sollten Sie sie mit der Registerkarte **Verknüpfungen** für die Zugriffsvorlage verwalten.

Schrittweise Anleitungen bezüglich der Verwaltung der Berechtigungsverbreitung finden Sie unter **Anleitungen/Verwalten von Zugriffsvorlagen/Synchronisieren von Berechtigungen nach Active Directory** in der ActiveRoles Server-Hilfe.

Verwalten von Berechtigungseinträgen in Active Directory

Auf der Registerkarte **Einheitliche Sicherheit** im erweiterten Detailfenster werden die einheitlichen Berechtigungseinträge von Active Directory für das ausgewählte sicherbare Objekt aufgelistet. Beispielsweise werden in der folgenden Abbildung auf der Registerkarte **Einheitliche Sicherheit** die Berechtigungseinträge für die Organisationseinheit aufgelistet, die in der Konsolenstruktur ausgewählt ist.



Indem Sie Informationen in den Spalten **Typ** und **Quelle** analysieren, können Sie erkennen, ob ein bestimmter Eintrag von ActiveRoles Server aus synchronisiert wird.

In der Spalte **Typ** sind die synchronisierten Einträge mit dem Symbol markiert. Dieses Symbol ändert sich zu , wenn die Synchronisierung des Eintrags ungültig oder nicht abgeschlossen ist. Wenn Sie beispielsweise einen synchronisierten Eintrag aus Active Directory löschen, erkennt ActiveRoles Server die Löschung und erstellt den Eintrag neu. Bis der Eintrag neu erstellt wird, ist er in der Spalte **Typ** mit dem Symbol markiert.

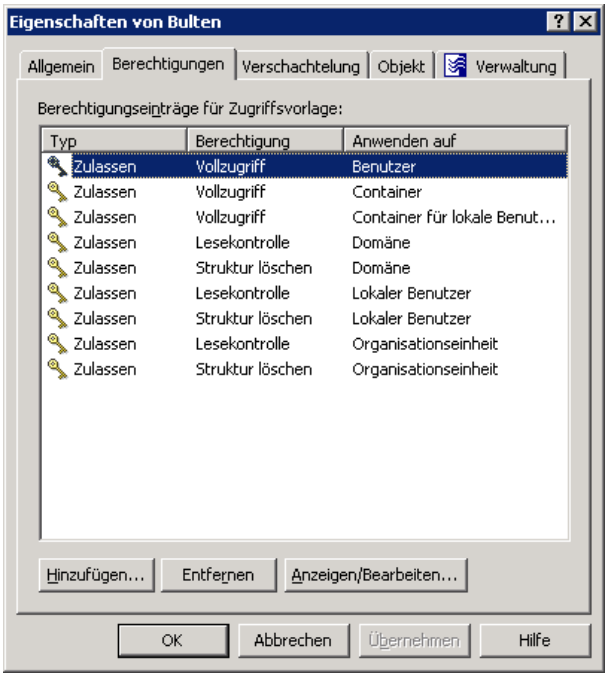
Für jeden synchronisierten Eintrag wird in der Spalte **Quelle** der Name der Zugriffsvorlage angezeigt, die die zu diesem Eintrag synchronisierten Berechtigungen definiert.

Auf der Registerkarte **Einheitliche Sicherheit** können Sie wie folgt Berechtigungseinträge verwalten: Klicken Sie mit der rechten Maustaste auf einen Eintrag, und klicken Sie dann auf **Einheitliche Sicherheit bearbeiten**. Dann wird das Dialogfeld **Berechtigungen** angezeigt, in dem Sie Berechtigungseinträge von Active Directory für das ausgewählte sicherbare Objekt hinzufügen, entfernen und ändern können.

Hinzufügen, Ändern und Entfernen von Berechtigungen

Wenn Sie Berechtigungen in einer Zugriffsvorlage hinzufügen, entfernen oder ändern, werden automatisch Berechtigungseinstellungen für alle Objekte geändert, auf die die Zugriffsvorlage angewendet wird (mit denen sie verknüpft ist), einschließlich derjenigen, die aufgrund von Vererbung von der Zugriffsvorlage betroffen sind.

Um Berechtigungen in einer Zugriffsvorlage hinzuzufügen, zu entfernen oder zu ändern, zeigen Sie das Dialogfeld **Eigenschaften** für die Zugriffsvorlage an, und zeigen Sie dann die Registerkarte **Berechtigungen** an:



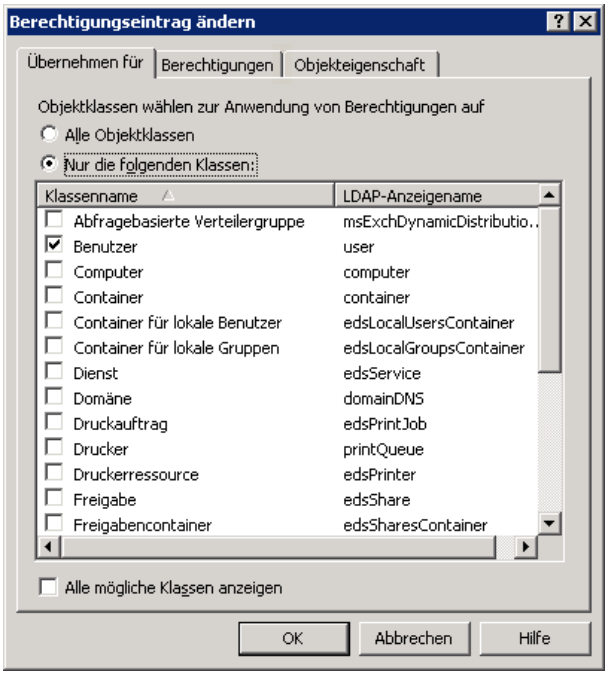
Auf der Registerkarte **Berechtigungen** werden Berechtigungseinträge aufgelistet, die in der Zugriffsvorlage definiert sind. Jeder Eintrag in der Liste schließt die folgenden Informationen ein:

- **Typ** Gibt an, ob die Berechtigung den Zugriff zulässt oder verweigert.
- **Berechtigung** Der Name der Berechtigung.
- **Anwenden auf** Der Typ der Objekte, die der Berechtigung unterliegen.

Um eine neue Berechtigung hinzuzufügen, klicken Sie auf **Hinzufügen** und schließen Sie den Assistenten Berechtigungseinträge hinzufügen wie unter „Erstellen von Zugriffsvorlagen" weiter oben in diesem Kapitel beschrieben ab.

Um Berechtigungen zu löschen, wählen Sie sie in der Liste **Berechtigungseinträge für Zugriffsvorlage** aus, und klicken Sie dann auf **Entfernen**.

Um eine Berechtigung zu ändern, wählen Sie sie in der Liste **Berechtigungseinträge für Zugriffsvorlage** aus, und klicken Sie dann auf **Anzeigen/Bearbeiten**. Damit wird das Dialogfeld **Berechtigungseintrag ändern** angezeigt, das der folgenden Abbildung ähnelt.



Auf den Registerkarten in diesem Dialogfeld können Sie die Berechtigungen nach Bedarf anpassen. Die Registerkarten sind identisch mit den Seiten im Assistenten Berechtigungseinträge hinzufügen, der unter „Erstellen von Zugriffsvorlagen" weiter oben in diesem Kapitel beschrieben ist.

Schrittweise Anleitungen bezüglich des Hinzufügens, Änderns und Entfernens von Berechtigungen zu/in/aus einer Zugriffsvorlage finden Sie in den Themen **Hinzufügen von Berechtigungen zu einer Zugriffsvorlage**, **Ändern von Berechtigungen in einer Zugriffsvorlage** und **Entfernen von Berechtigungen aus einer Zugriffsvorlage** unter der Überschrift **Anleitungen/Verwalten von Zugriffsvorlagen** in der ActiveRoles Server-Hilfe.

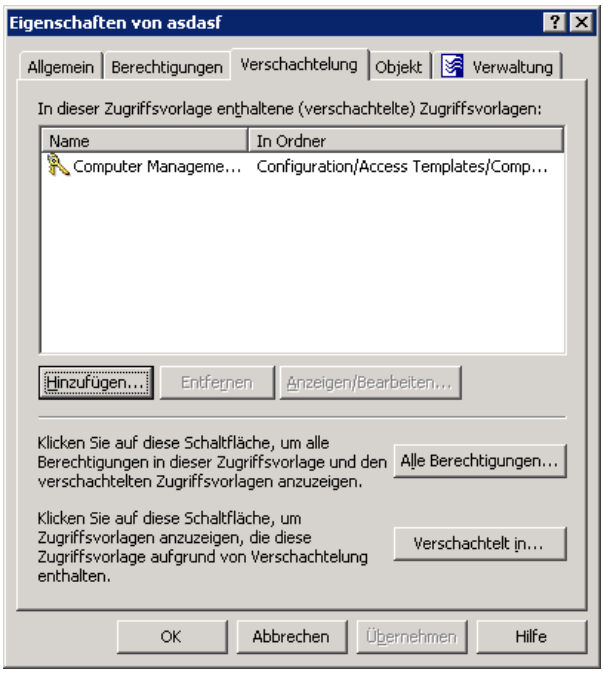
Schachteln von Zugriffsvorlagen

ActiveRoles Server ermöglicht das Definieren von Berechtigungen in einer Zugriffsvorlage durch Einschließen (Schachteln) anderer Zugriffsvorlagen. Dies reduziert die erforderliche Arbeit für das Erstellen einer neuen Zugriffsvorlage, die einer vorhandenen ähnelt. Statt eine vorhandene Vorlage durch Hinzufügen neuer Berechtigungen zu ändern, können Sie sie in eine neue Zugriffsvorlage schachteln.

Diese Funktion vereinfacht die Verwaltung von Zugriffsvorlagen durch Wiederverwenden der vorhandenen vordefinierten oder benutzerdefinierten Zugriffsvorlagen. Wenn Sie beispielsweise der vordefinierten Zugriffsvorlage für das Help Desk Berechtigungen hinzufügen möchten, können Sie eine neue Zugriffsvorlage erstellen, die Help Desk-Zugriffsvorlage in die neue Zugriffsvorlage schachteln und der neuen Zugriffsvorlage nach Bedarf Berechtigungen hinzufügen.

Um Zugriffsvorlagen in eine gegebene Zugriffsvorlage zu schachteln, verwenden Sie im Dialogfeld **Eigenschaften** für diese Zugriffsvorlage die Registerkarte **Verschachtelung**.

Auf der Registerkarte **Verschachtelung** werden alle Zugriffsvorlagen aufgelistet, die in die ausgewählte Zugriffsvorlage eingeschlossen (geschachtelt) sind, wie in der folgenden Abbildung:



Jeder Eintrag in der Liste stellt die folgenden Informationen bereit:

- **Name** Den Namen der verschachtelten Zugriffsvorlage.
- **In Ordner** Den Pfad zu dem Container, der die geschachtelte Zugriffsvorlage enthält.

Sie können die Liste auf der Registerkarte **Verschachtelung** mit Hilfe der Schaltflächen unter der Liste wie folgt verwalten:

- **Hinzufügen** Klicken Sie auf diese Schaltfläche, um Zugriffsvorlagen auszuwählen, die Sie in die zu verwaltende Zugriffsvorlage schachteln möchten.
- **Entfernen** Wählen Sie Zugriffsvorlagen in der Liste aus und klicken Sie auf diese Schaltfläche, um sie aus der zu verwaltenden Zugriffsvorlage zu entfernen.
- **Anzeigen/Bearbeiten** Wählen Sie eine Zugriffsvorlage in der Liste aus, und klicken Sie auf diese Schaltfläche, um die ausgewählte Zugriffsvorlage anzuzeigen oder zu ändern.

Über die Registerkarte **Verschachtelung** können Sie auch auf die folgenden Informationen zugreifen:

- **Alle Berechtigungen** Zeigt alle Berechtigungen in der Zugriffsvorlage an, einschließlich derjenigen, die aus den geschachtelten Zugriffsvorlagen stammen.
- **Verschachtelt in** Zeigt eine Liste der Zugriffsvorlagen an, in die die Zugriffsvorlage aufgrund der Schachtelung eingeschlossen ist.

Schrittweise Anleitungen bezüglich der Verwaltung der Verschachtelung von Zugriffsvorlagen finden Sie unter **Anleitungen/Verwalten von Zugriffsvorlagen/Verwalten von verschachtelten Zugriffsvorlagen** in der ActiveRoles Server-Hilfe.

Kopieren einer Zugriffsvorlage

Mit der ActiveRoles Server-Konsole können Sie Kopien von Zugriffsvorlagen erstellen. Mit dieser Funktion können Sie vorhandene Zugriffsvorlagen wieder verwenden. Wenn Sie beispielsweise eine vordefinierte Zugriffsvorlage ändern möchten, können Sie sie kopieren und dann die Kopie nach Bedarf ändern.

Zum Erstellen einer Kopie einer Zugriffsvorlage klicken Sie mit der rechten Maustaste auf die Zugriffsvorlage, und klicken Sie dann auf **Kopieren**. Dann wird der Assistent zum Kopieren des Objekts – Zugriffsvorlage geöffnet. Geben Sie einen Namen und eine Beschreibung für die Kopie ein, und klicken Sie dann auf **Weiter**.

Auf der nächsten Seite des Assistenten wird eine Liste von Berechtigungseinträgen angezeigt. Standardmäßig schließt die Liste alle in der ursprünglichen Zugriffsvorlage definierten Einträge ein. Sie können die Liste auf dieselbe Weise ändern wie auf der Registerkarte **Berechtigungen** im Dialogfeld **Eigenschaften** für eine Zugriffsvorlage (siehe „Hinzufügen, Ändern und Entfernen von Berechtigungen" weiter oben in diesem Kapitel).

Nach Abschluss der Arbeit mit der Liste der Berechtigungseinträge klicken Sie auf **Weiter** und dann auf **Fertig stellen**, um den Assistenten abzuschließen.

Schrittweise Anleitungen bezüglich der Erstellung einer Kopie einer Zugriffsvorlage finden Sie unter **Anleitungen/Verwalten von Zugriffsvorlagen/Kopieren von Zugriffsvorlagen** in der ActiveRoles Server-Hilfe.

Exportieren und Importieren von Zugriffsvorlagen

Mit der ActiveRoles Server-Konsole können Sie Zugriffsvorlagen in eine XML-Datei exportieren und sie dann aus dieser Datei importieren, um eine andere Instanz von ActiveRoles Server aufzufüllen. Die Export- und Importvorgänge stellen eine Möglichkeit bereit, Zugriffsvorlagen von einer Testumgebung in eine Produktionsumgebung zu verschieben und umgekehrt.

Wenn Sie Zugriffsvorlagen exportieren und dann importieren, werden nur Berechtigungseinträge übertragen. Die Zugriffsvorlagenverknüpfungen sind nicht im Export-Import-Vorgang eingeschlossen. Daher müssen Sie sie nach Abschluss des Vorgangs manuell neu konfigurieren.

Um Zugriffsvorlagen zu exportieren, wählen Sie sie aus, klicken Sie mit der rechten Maustaste auf die Auswahl und wählen Sie dann **Alle Aufgaben | Exportieren**. Geben Sie im Dialogfeld **Objekte exportieren** die Datei an, in der Sie die Daten speichern möchten, und klicken Sie dann auf **Speichern**.

Zum Importieren von Zugriffsvorlagen klicken Sie mit der rechten Maustaste auf den Container, in dem Sie die Zugriffsvorlagen ablegen möchten, und klicken Sie dann auf **Importieren**. Wählen Sie im Dialogfeld **Verzeichnisobjekte importieren** die Datei aus, in die die Zugriffsvorlagen exportiert wurden, und klicken Sie dann auf **Öffnen**.

Schrittweise Anleitungen bezüglich des Exports und Imports von Zugriffsvorlagen finden Sie in den Themen **Exportieren einer Zugriffsvorlage** und **Importieren einer Zugriffsvorlage** unter der Überschrift **Anleitungen/Verwalten von Zugriffsvorlagen** in der ActiveRoles Server-Hilfe.

Umbenennen einer Zugriffsvorlage

Zum Umbenennen einer Zugriffsvorlage klicken Sie mit der rechten Maustaste auf die Zugriffsvorlage, und klicken Sie dann auf **Umbenennen**. Geben Sie den neuen Namen ein, und drücken Sie dann die Eingabetaste.

Das Umbenennen einer Zugriffsvorlage hat keine Auswirkungen auf ihre Verknüpfungen. Der Grund ist, dass auf Zugriffsvorlagen über unveränderliche Bezeichner statt über ihre Namen verwiesen wird.

Schrittweise Anleitungen bezüglich der Umbenennung einer Zugriffsvorlage finden Sie unter **Anleitungen/Verwalten von Zugriffsvorlagen/Umbenennen von Zugriffsvorlagen** in der ActiveRoles Server-Hilfe.

Löschen einer Zugriffsvorlage

Um eine Zugriffsvorlage zu löschen, müssen Sie zuerst wie folgt alle Verweise auf diese löschen:

- Löschen Sie die Verknüpfungen zur Zugriffsvorlage (siehe „Verwalten von Zugriffsvorlagenverknüpfungen" weiter oben in diesem Kapitel).
- Entfernen Sie die Zugriffsvorlage aus allen Zugriffsvorlagen, unter denen die Zugriffsvorlage verschachtelt ist (siehe „Verschachteln von Zugriffsvorlagen" weiter oben in diesem Kapitel).

Dann können Sie den Löschvorgang wie folgt ausführen: Klicken Sie mit der rechten Maustaste auf die Zugriffsvorlage, und klicken Sie dann auf **Löschen**.

Schrittweise Anleitungen bezüglich des Löschens einer Zugriffsvorlage finden Sie unter **Anleitungen/Verwalten von Zugriffsvorlagen/Löschen von Zugriffsvorlagen** in der ActiveRoles Server-Hilfe.

Verwendungsbeispiele

In diesem Abschnitt werden Szenarien diskutiert, die Ihnen das Verstehen und die Verwendung der rollenbasierten Verwaltungsfunktionen erleichtern, die in ActiveRoles Server zur Verfügung stehen. Folgende Szenarien werden erörtert:

- Implementieren eines Help Desk
- Implementieren der Selbstverwaltung

Szenario 1: Implementieren eines Help Desk

In diesem Szenario wird gezeigt, wie Sie mit Hilfe einer Zugriffsvorlage einem Help Desk-Service die Ausführung täglicher Vorgänge für Benutzerkonten ermöglichen, z.B. das Zurücksetzen von Kennwörtern, Anzeigen von Benutzereigenschaften sowie das Sperren und Entsperren von Benutzerkonten.

In dem Szenario kommt auch eine Gruppe vor, die Help Desk-Operatoren enthalten soll. Die Zugriffsvorlage wird angewendet, sodass die Gruppe als Trustee ausgewählt wird und die Help Desk-Operatoren somit Administratorrechte erhalten. Nach der Vorbereitung der Zugriffsvorlage und der Gruppe können Sie eine Help Desk-Verwaltung im Unternehmen implementieren.

Angenommen, Sie möchten das Help Desk autorisieren, Benutzerkonten in der Organisationseinheit **Vertrieb** zu verwalten. Führen Sie zum Implementieren dieses Szenarios die folgenden Schritte aus:

1. Bereiten Sie die Zugriffsvorlage **Help Desk** vor, in der die Berechtigungen für Help Desk-Operatoren in Bezug auf Benutzerkonten definiert sind.
2. Erstellen Sie die Gruppe **Help Desk**, die die Help Desk-Operatoren enthalten soll, und füllen Sie sie auf.
3. Wenden Sie die Zugriffsvorlage **Help Desk** auf die Organisationseinheit **Vertrieb** an, und wählen Sie dabei die Gruppe **Help Desk** als Trustee aus.

Als Ergebnis dieser Schritte wird jedes Mitglied der Gruppe **Help Desk** dazu autorisiert, Verwaltungsaufgaben für Benutzerkonten in der Organisationseinheit **Vertrieb** auszuführen. Die Zugriffsvorlage **Help Desk** bestimmt den Bereich dieser Aufgaben.

In den folgenden Abschnitten werden alle diesen Schritte ausführlich beschrieben.

Schritt 1: Vorbereiten einer Zugriffsvorlage für das Help Desk

Für dieses Szenario können Sie die vordefinierte Zugriffsvorlage **Users – Help Desk** im Ordner **Configuration/Access Templates/Active Directory** verwenden. Die Zugriffsvorlage **Users – Help Desk** gibt die notwendigen Berechtigungen zum Zurücksetzen von Benutzerkennwörtern, zum Entsperren von Benutzerkonten sowie zum Anzeigen ihrer Eigenschaften an.

Um Berechtigungen zur Zugriffsvorlage **Users – Help Desk** hinzuzufügen oder aus ihr zu entfernen, müssen Sie zuerst eine Kopie dieser Zugriffsvorlage erstellen und diese Kopie dann ändern und anwenden.

Für dieses Szenario wird angenommen, dass Sie die vordefinierte Zugriffsvorlage **Users – Help Desk** anwenden.

Schritt 2: Erstellen einer Gruppe für das Help Desk

Um eine Gruppe zu erstellen, klicken Sie mit der rechten Maustaste auf eine Organisationseinheit in der Konsolenstruktur, wählen Sie dann **Neu | Gruppe** aus und befolgen Sie anschließend die Anweisungen des Assistenten „Neues Objekt – Gruppe". Der Assistent schließt die Seite ein, auf der Sie der gerade erstellten Gruppe Mitglieder (Help Desk-Operatoren) hinzufügen können.

Schrittweise Anleitungen bezüglich der Erstellung von Gruppen finden Sie unter **Anleitungen/Verwalten von Gruppen/Erstellen einer Gruppe** in der ActiveRoles Server-Hilfe.

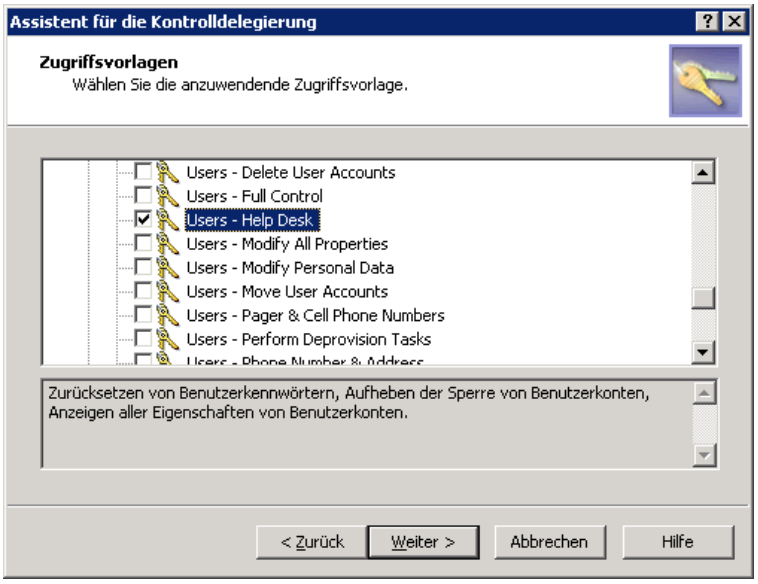
Schritt 3: Anwenden der Zugriffsvorlage für das Help Desk

Sie können die Zugriffsvorlage anwenden, indem Sie den Assistenten „Delegation der Kontrolle" verwenden:

Starten Sie zunächst den Assistenten wie folgt für die Organisationseinheit **Vertrieb**: Klicken Sie mit der rechten Maustaste auf die Organisationseinheit, klicken Sie auf **Kontrolle delegieren**, und klicken Sie dann im Fenster **ActiveRoles Server-Sicherheit** auf die Schaltfläche **Hinzufügen**.

Fügen Sie dann auf der Seite **Benutzer oder Gruppen** des Assistenten die Gruppe **Help Desk** zu der Liste hinzu.

Erweitern Sie dann auf der Seite **Zugriffsvorlagen** des Assistenten den Eintrag **Access Templates | Active Directory** und aktivieren Sie das Kontrollkästchen neben **Users – Help Desk**, wie in der folgenden Abbildung gezeigt.


Assistent für die Kontrolldelegierung
Zugriffsvorlagen
Wählen Sie die anzuwendende Zugriffsvorlage.
Users - Delete User Accounts
Users - Full Control
Users - Help Desk
Users - Modify All Properties
Users - Modify Personal Data
Users - Move User Accounts
Users - Pager & Cell Phone Numbers
Users - Perform Deprovision Tasks
Zurücksetzen von Benutzerkennwörtern, Aufheben der Sperre von Benutzerkonten, Anzeigen aller Eigenschaften von Benutzerkonten.
< Zurück
Weiter >
Abbrechen
Hilfe

Klicken Sie auf **Weiter**, und akzeptieren Sie die Standardeinstellungen des Assistenten. Klicken Sie auf der Abschlussseite auf **Fertig stellen**. Klicken Sie zum Schluss auf **OK**, um das Fenster **ActiveRoles Server-Sicherheit** zu schließen.

Weitere Informationen über den Assistenten „Delegation der Kontrolle" finden Sie unter „Anwenden von Zugriffsvorlagen" weiter oben in diesem Kapitel.

Szenario 2: Implementieren der Selbstverwaltung

In diesem Szenario wird die Verwendung einer Zugriffsvorlage gezeigt, die Benutzern das Ändern bestimmter Teile ihrer persönlichen Daten in Active Directory ermöglicht.

Das Web-Interface von ActiveRoles Server stellt die Seite für die Selbstverwaltung bereit, über die Benutzerkonten verwaltet werden können. Auf der Seite werden den Benutzern ihre persönlichen Daten angezeigt, z.B. Vor- und Nachnamen, Adressdaten, Telefonnummern und andere Daten. Standardmäßig sind Benutzer des Web-Interface nur zum Anzeigen ihrer persönlichen Daten autorisiert. Damit die Benutzer ihre persönlichen Daten auch ändern können, müssen Sie ihnen zusätzliche Berechtigungen erteilen.

Angenommen, Sie möchten die Benutzer in der Organisationseinheit **Vertrieb** zur Ausführung von Selbstverwaltung autorisieren. Führen Sie zum Implementieren dieses Szenarios die folgenden Schritte aus:

1. Bereiten Sie die Zugriffsvorlage **Self-Administration** vor, in der die geeigneten Berechtigungen in Bezug auf Benutzerkonten definiert sind.
2. Wenden Sie die Zugriffsvorlage **Self-Administration** auf die Organisationseinheit **Vertrieb** an, und wählen Sie dabei das Objekt **Selbst** als Trustee aus.

Nach Ausführung dieser Schritte sind Benutzer aus der Organisationseinheit **Vertrieb** dazu autorisiert, Selbstverwaltungsaufgaben für ihre persönlichen Konten auszuführen. Die Zugriffsvorlage **Self-Administration** bestimmt, welche Daten die Benutzer ändern können. Benutzer können mit Hilfe der Selbstverwaltungsseite ihre persönlichen Daten verwalten. Weitere Informationen über die Selbstverwaltungsseite finden Sie im ActiveRoles Server Web-Interface – Benutzerhandbuch.

In den folgenden Abschnitten werden die Schritte in diesem Szenario detailliert erörtert.

Schritt 1: Vorbereiten einer Zugriffsvorlage für die Selbstverwaltung

Für dieses Szenario können Sie die vordefinierte Zugriffsvorlage **Self-Service – My Account Management** im Ordner **Configuration/Access Templates/Active Directory** verwenden. Diese Zugriffsvorlage gibt die notwendigen Berechtigungen zum Anzeigen grundlegender Benutzereigenschaften und zum Ändern von Telefonnummern an.

Um Berechtigungen zur Zugriffsvorlage **Self-Service – My Account Management** hinzuzufügen oder aus ihr zu entfernen, müssen Sie zuerst eine Kopie dieser Zugriffsvorlage erstellen und diese Kopie dann ändern und anwenden.

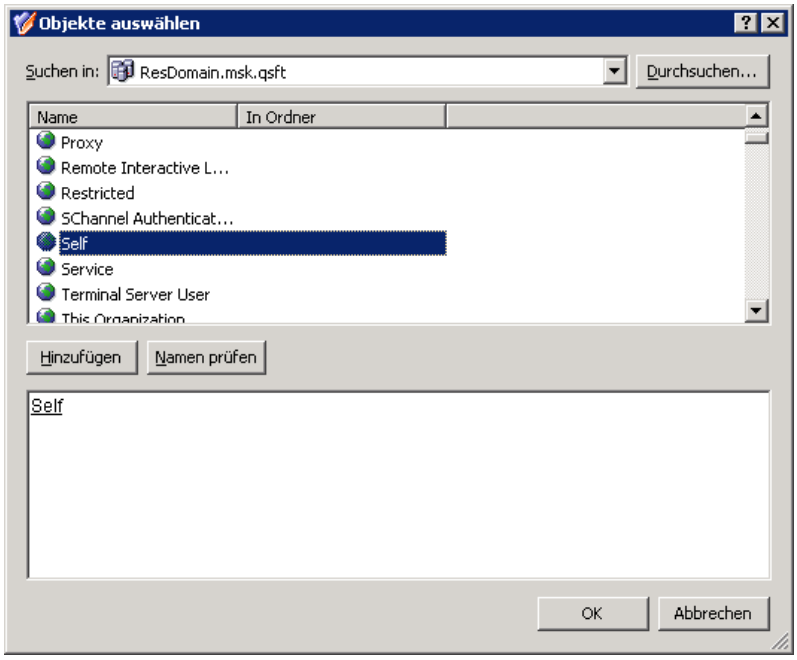
Für dieses Szenario wird angenommen, dass Sie die vordefinierte Zugriffsvorlage **Self-Service – My Account Management** anwenden.

Schritt 2: Anwenden der Zugriffsvorlage für die Selbstverwaltung

Sie können die Zugriffsvorlage anwenden, indem Sie den Assistenten „Delegation der Kontrolle" verwenden:

Starten Sie zunächst den Assistenten wie folgt für die Organisationseinheit **Vertrieb**: Klicken Sie mit der rechten Maustaste auf die Organisationseinheit, klicken Sie auf **Kontrolle delegieren**, und klicken Sie dann im Fenster **ActiveRoles Server-Sicherheit** auf die Schaltfläche **Hinzufügen**.

Klicken Sie dann auf der Seite **Benutzer oder Gruppen** des Assistenten auf die Schaltfläche **Hinzufügen**. Wählen Sie im Fenster **Objekte auswählen** das Objekt **Self** aus (wie in der folgenden Abbildung gezeigt), klicken Sie auf **Hinzufügen** und dann auf **OK**.



Erweitern Sie als nächstes auf der Seite **Zugriffsvorlagen** des Assistenten die Einträge **Access Templates | Active Directory** und aktivieren Sie das Kontrollkästchen neben **Self-Service – My Account Management**.

Klicken Sie auf **Weiter**, und akzeptieren Sie die Standardeinstellungen des Assistenten. Klicken Sie auf der Abschlussseite auf **Fertig stellen**. Klicken Sie zum Schluss auf **OK**, um das Fenster **ActiveRoles Server-Sicherheit** zu schließen.

Weitere Informationen über den Assistenten „Delegation der Kontrolle" finden Sie unter „Anwenden von Zugriffsvorlagen" weiter oben in diesem Kapitel.

5

Regelbasierte automatische Bereitstellung und Deprovisionierung

- Richtlinienobjekte
- Verwaltungsaufgaben für Richtlinienobjekte
- Konfigurationsaufgaben für Richtlinien
- Überprüfen der Richtlinieneinhaltung
- Deprovisionieren von Benutzern oder Gruppen
- Wiederherstellen von deprovisionierten Benutzern oder Gruppen
- Richtlinie zur Vermeidung einer Containerlöschung
- Erweiterungsfähigkeit von Richtlinien

Richtlinienobjekte

Active Directory ermöglicht eine sehr granuläre Delegierung der Kontrolle. Die Möglichkeit, den Zugriff einzuschränken, reicht jedoch möglicherweise nicht aus.

Viele Aktivitäten bei der Verzeichnisverwaltung folgen einem vordefinierten Workflow. Bei diesem Workflow wird eine Reihe von Aufgaben in einer bestimmten Reihenfolge ausgeführt. Administratoren und andere Mitarbeiter müssen wiederholt fast identische Aufgaben ausführen. Einige Beispiele: Erstellen von Benutzerkonten, Zurücksetzen von Kennwörtern, Deaktivieren inaktiver Benutzerkonten, Durchsetzen von Namenskonventionen für Benutzer.

ActiveRoles Server ist eine richtlinienbasierte Verwaltungslösung und erfüllt die Anforderungen heutiger Unternehmen. Die Durchsetzung administrativer Richtlinien in ActiveRoles Server reduziert die Arbeitslast für die Verwaltung erheblich, verbessert die Netzwerksicherheit und stellt unternehmensweite Konsistenz sicher. Durch die Automatisierung des Verwaltungsworkflows wird die Zeit für die Ausführung von Aufgaben deutlich reduziert, und einige Aufgaben können völlig eliminiert werden. Außerdem wird die Fehleranfälligkeit minimiert, die Notwendigkeit von Nacharbeiten wird reduziert, und zusammengehörige Aktionen werden in einem einzelnen Batch kombiniert.

Mit ActiveRoles Server können Sie angeben, was bei jeder Änderung, Erstellung oder Löschung von Verzeichnisobjekten wann und wie geändert werden muss. Außerdem können Sie ActiveRoles Server so konfigurieren, dass nur Datenänderungen akzeptiert werden, die bestimmte Formatierungsanforderungen erfüllen. So können Sie die im Verzeichnis gespeicherten Daten besser steuern.

Wenn Sie beispielsweise ein Benutzerkonto für einen neuen Mitarbeiter erstellen, kann ActiveRoles Server automatisch Informationen aus einer Datenbank der Personalabteilung abrufen, sie in den Eigenschaften des Benutzerkontos als Standardinformationen verwenden, einen Stammordner und eine Stammfreigabe erstellen und das neue Konto den notwendigen Gruppen hinzufügen. Außerdem kann das Programm ein Exchange-Postfach erstellen und es den relevanten Verteilungslisten hinzufügen. Das gesamte Vorgehen bedeutet eine einzige Aufgabe, während es ohne ActiveRoles Server zehn oder mehr Aufgaben darstellen kann.

Dank der Möglichkeit, administrative Richtlinien durchzusetzen und Verwaltungsworkflows zu automatisieren, spart ActiveRoles Server nicht nur Zeit, sondern erhält auch Netzwerkobjekte in einem konsistenten Zustand im Verhältnis zu den einzelnen definierten Richtlinien. Dies betrifft wichtige Fragen der Sicherheit, Verwendbarkeit und Integrität, die für die Verwaltung von Netzwerkobjektdaten von zentraler Bedeutung sind.

In ActiveRoles Server werden administrative Richtlinien mit Hilfe von Richtlinienobjekten definiert. Dabei handelt es sich um Sammlungen von Richtlinien. Richtlinienobjekte definieren das Verhalten des Systems bei der Erstellung, Änderung oder Löschung von Verzeichnisobjekten.

Sie können ein Richtlinienobjekt erstellen, das beliebig viele unterschiedliche Richtlinien enthält, wie beispielsweise eine Formatüberprüfung, Generierungsregeln für die Werte von Objektattributen, Skripts zur Ergänzung administrativer Vorgänge, die automatische Erstellung von Benutzerpostfächern auf vorgegebenen Exchange-Servern, eine automatische Erstellung von Stammordnern und Stammfreigaben für Benutzer sowie Neuzuordnung eines Objekts zu einem angegebenen Container, wenn es bestimmte Kriterien erfüllt.

ActiveRoles Server stellt umfangreiche Automatisierungsfunktionen für administrative Prozesse bereit. Richtlinienobjekte können anpassbare Skripts vor oder nach der Ausführung eines beliebigen spezifischen Tasks ausführen, und mehrere Tasks können in einen Vorgang kombiniert werden. Diese Funktionalität reduziert den Zeitaufwand für Verwaltungsaufgaben wesentlich und minimiert Fehler.

Mit Hilfe von Richtlinienobjekten automatisiert ActiveRoles Server die Aufgaben der Bereitstellung für Benutzer, verringert so Ihre Arbeitslast für die Verwaltung und ermöglicht es, neuen Benutzern schneller die benötigten Ressourcen bereitzustellen. Das Programm automatisiert außerdem auch die erneute Bereitstellung und die Deprovision. Wenn der Zugriff eines Benutzers geändert oder entfernt werden muss, werden Aktualisierungen in Active Directory, Exchange und Windows also automatisch vorgenommen. Dies reduziert die Arbeitslast für die Verwaltung und ermöglicht Benutzern eine schnellere, größere Produktivität.

Um Ihnen das Konfigurieren und Anwenden von Richtlinienobjekten zu erleichtern, werden sie in zwei Kategorien eingeteilt:

- **Bereitstellungsrichtlinienobjekte** Mit diesen Objekten werden Bereitstellungsregeln angegeben. Dazu gehören Regeln zur Auffüllung und Überprüfung von Verzeichnisdaten, zur Erstellung von Ressourcen wie Stammordnern und Postfächern sowie zur Bereitstellung eines Ressourcenzugriffs.
- **Deprovisionsrichtlinienobjekte** Mit diesen Objekten werden Regeln für die Rücknahme von Bereitstellungen angegeben. Dazu gehören Regeln zum Entfernen von Benutzerkonten und E-Mail-Konten, Stammordnern, Sicherheits- und Verteilungslisten sowie des Anwendungszugriffs in Reaktion auf Anforderungen zur Deprovision von Benutzern oder Gruppen.

Sie können beliebig viele Richtlinienobjekte in jeder der beiden Kategorien erstellen und anwenden.

Bereitstellungsrichtlinienobjekte

Bereitstellungsrichtlinienobjekte ermöglichen die Konfiguration und Anwendung der folgenden Richtlinien.

RICHTLINIE	BESCHREIBUNG
Erzeugung von Benutzeranmeldenamen	Diese Richtlinie generiert einen Benutzer-Anmeldenamen (Prä-Windows 2000) für ein zu erstellendes Benutzerkonto. Sie können sie für Folgendes konfigurieren: • Hinzufügen einer Eindeutigkeitszahl zum generierten Anmeldenamen • Anwenden mehrerer Regeln für das Generieren eines Anmeldenamens • Ermöglichen, dass während des Benutzererstellungsprozesses ein Anmeldename manuell angegeben wird Indem Sie diese Optionen kombinieren, können Sie sicherstellen, dass der Benutzer-Anmeldename (Prä-Windows 2000) eindeutig ist. Dies ist eine Schemaanforderung in Active Directory.
E-Mail-Aliaserzeugung	Mit dieser Richtlinie wird sichergestellt, dass für neu erstellte Benutzerkonten die richtigen E-Mail-Aliase eingerichtet sind. Sie können sie für die Generierung von Aliasen konfigurieren, denen Folgendes zugrunde liegt: • Vorher ausgewählte Benutzereigenschaften, wie Vor- und Nachnamen • Eine benutzerdefinierte Auswahl von Eigenschaften, nicht auf Benutzereigenschaften eingeschränkt Mit dieser Richtlinie kann jeder Alias eindeutig gemacht werden, indem ihm eine Eindeutigkeitszahl hinzugefügt wird.

RICHTLINIE	BESCHREIBUNG
Automatische Bereitstellung von Exchange-Postfächern	Mit dieser Richtlinie wird sichergestellt, dass Benutzerpostfächer in geeigneten Postfachspeichern oder Datenbanken erstellt werden. Sie können sie für Folgendes konfigurieren: • Bestimmen der Postfachspeicher oder Datenbanken, in denen die Erstellung von Postfächern zulässig ist • Anwenden einer Regel für das Verteilen von Postfächern auf mehrere Speicher oder Datenbanken Mit dieser Richtlinie können Sie Postfächer im Kreisverfahren verteilen oder jeweils im Speicher oder in der Datenbank mit den wenigsten Postfächern ablegen.
Automatische Bereitstellung der Gruppenmitgliedschaft	Mit dieser Richtlinie wird sichergestellt, dass Benutzerkonten zu geeigneten Gruppen gehören. Sie können sie für Folgendes konfigurieren: • Hinzufügen von Benutzerkonten zu bestimmten Gruppen • Entfernen von Benutzerkonten aus bestimmten Gruppen Sie können Gruppen auswählen und Kriterien einrichten. Die Richtlinie fügt ein Benutzerkonto zu den ausgewählten Gruppen hinzu oder entfernt es daraus, abhängig davon, ob das Benutzerkonto die angegebenen Kriterien erfüllt. Die Richtlinie kann auch auf Verzeichnisobjekte angewendet werden, die keine Benutzerkonten sind.
Automatische Bereitstellung des Stammordners	Diese Richtlinie führt Bereitstellungsaufgaben aus, die notwendig sind, um Benutzerkonten Stammordner und Stammfreigaben zuzuweisen. Sie können sie für Folgendes konfigurieren: • Erstellen von Stammordnern für neu erstellte Benutzerkonten • Umbenennen von Stammordnern beim Umbenennen von Benutzerkonten Sie können den Server angeben, auf dem Stammordner und -freigaben erstellt werden sollen, Namenskonventionen für Stammordner und -freigaben bestimmen sowie Zugriffsrechte für die neu erstellten Stammordner und -freigaben konfigurieren.
Erzeugung und Validierung von Eigenschaften	Diese Richtlinie generiert und überprüft Verzeichnisdaten, z.B. Benutzereigenschaften. Sie können sie für Folgendes konfigurieren: • Auffüllen des Verzeichnisses mit Standarddaten • Ausführen von Datengültigkeitsprüfungen bei Verzeichnisaktualisierungen Sie können angeben, wie die Richtlinie Verzeichnisdaten standardmäßig generieren soll und welche Überprüfungskriterien angewendet werden müssen, um sicherzustellen, dass die Verzeichnisdaten Ihren Unternehmensstandards entsprechen.
Skriptausführung	Diese Richtlinie führt auf Anforderung ein Skript aus, mit dem bestimmte Vorgänge ausgeführt werden, wie die Erstellung oder Aktualisierung von Benutzerkonten. Mit Skripts können Sie folgende Vorgänge ausführen: • Auslösen zusätzlicher Aktionen für die Benutzerbereitstellung • Regulierung von Datenformaten und -anforderungen • Automatisierung von Verwaltungsaufgaben Sie können ein benutzerdefiniertes Skript mit einem administrativen Vorgang verknüpfen und dem Skript die Kontrolle geben, wenn der Vorgang angefordert wird oder nachdem er abgeschlossen wurde.

Deprovisionsrichtlinienobjekte

Richtlinienobjekte zur Deprovision ermöglichen die Konfiguration und Anwendung der folgenden Richtlinien.

RICHTLINIE	BESCHREIBUNG
Benutzerkonto-deprovisionierung	Bei der Deprovision für einen Benutzer ändert diese Richtlinie das Benutzerkonto so, dass der Benutzer sich nicht mehr anmelden kann. Sie können diese Richtlinie für Folgendes konfigurieren: • Deaktivieren des Benutzerkontos • Festlegen des Kennworts des Benutzers auf einen zufälligen Wert • Festlegen der Anmeldenamen des Benutzers auf zufällige Werte • Umbenennen des Benutzerkontos Sie können auch Kontoeigenschaften auswählen und diese Richtlinie so konfigurieren, dass sie sie bei der Verarbeitung einer Rücknahmeanforderung für eine Bereitstellung aktualisiert.
Entfernen der Gruppenmitgliedschaft	Bei der Deprovision für einen Benutzer entfernt diese Richtlinie das Benutzerkonto aus Gruppen. Sie können diese Richtlinie so konfigurieren, dass sie das Konto aus Sicherheitsgruppen, E-Mail-fähigen Gruppen oder beidem entfernt. Bei dieser Richtlinie werden sowohl Verteilergruppen als auch E-Mail-fähige Sicherheitsgruppen zusammen als E-Mail-fähige Gruppen bezeichnet. Sie können auch die Gruppen auswählen, aus denen diese Richtlinie das Benutzerkonto nicht entfernen soll, oder die Richtlinie so konfigurieren, dass sie das Benutzerkonto aus keiner Sicherheitsgruppe und keiner E-Mail-fähigen Gruppe entfernt.
Benutzerkonto-Verschiebung	Bei der Deprovision für einen Benutzer verschiebt diese Richtlinie das Benutzerkonto an einen anderen Ort. Sie können die Organisationseinheit auswählen, in die die Richtlinie das Konto verschieben soll. Sie können die Richtlinie auch so konfigurieren, dass sie bei der Deprovision für einen Benutzer die Benutzerkonten nicht verschiebt.
Deprovisionierung des Exchange-Postfachs	Bei der Deprovision für einen Benutzer nimmt diese Richtlinie die erforderlichen Änderungen vor, um die Bereitstellung von Microsoft Exchange-Ressourcen für diesen Benutzer aufzuheben. Sie können diese Richtlinie für Folgendes konfigurieren: • Ausblenden des Postfachs aus der globalen Adressliste • Verhindern, dass Unzustellbarkeitsberichte gesendet werden • Vorgesetztem des Benutzers Vollzugriff auf das Postfach des Benutzers gewähren • Ausgewählten Benutzern oder Gruppen Vollzugriff auf das Postfach des Benutzers gewähren • Verweigern der Nachrichtenweiterleitung an alternative Empfänger • Weiterleiten aller eingehenden Nachrichten an den Vorgesetzten des Benutzers
Stammordner-Deprovisionierung	Bei der Deprovision für einen Benutzer nimmt diese Richtlinie Änderungen vor, die verhindern, dass der Benutzer auf den eigenen Stammordner zugreift. Sie können diese Richtlinie für Folgendes konfigurieren: • Entfernen der Berechtigungen des Benutzers für den Stammordner • Gewähren von Lesezugriff auf den Stammordner des Benutzers an den Vorgesetzten des Benutzers • Gewähren von Lesezugriff auf den Stammordner des Benutzers für ausgewählte Benutzer oder Gruppen • Festlegen eines ausgewählten Benutzers oder einer ausgewählten Gruppe als Besitzer des Stammordners des Benutzers • Den Stammordner beim Löschen des Benutzerkontos löschen

RICHTLINIE	BESCHREIBUNG
Permanentes Löschen von Benutzerkonten	Bei der Deprovisionierung für einen Benutzer plant diese Richtlinie die Löschung des Benutzerkontos. Sie können die Anzahl der Tage (den Wartezeitraum) bis zur Löschung des Kontos angeben. Eine andere Option ist das Löschen der deprovisionierten Benutzerkonten (sofortiges Verschieben in den Active Directory-Papierkorb). Sie können diese Richtlinie auch so konfigurieren, dass deprovisionierte Benutzerkonten nicht automatisch gelöscht werden.
Gruppenobjekt-Deprovisionierung	Diese Richtlinie nimmt bei der Deprovisionierung einer Gruppe Änderungen am Gruppenobjekt in Active Directory vor, um die Verwendung der Gruppe zu vermeiden. Sie können diese Richtlinie für Folgendes konfigurieren: • Gruppe in der globalen Adressliste (GAL) ausblenden • Gruppentyp von „Sicherheit" in „Verteilung" ändern • Gruppe umbenennen • Mitglieder aus der Gruppe entfernen • Jegliche andere Eigenschaften des Gruppenobjekts ändern oder löschen
Gruppenobjekt-Verschiebung	Bei der Deprovisionierung einer Gruppe verschiebt diese Richtlinie das Gruppenobjekt in einen anderen Container in Active Directory. Sie können die Organisationseinheit wählen, in die die Richtlinie das Gruppenobjekt verschieben soll.
Dauerhaftes Löschen des Gruppenobjekts	Bei der Deprovisionierung einer Gruppe plant diese Richtlinie die Löschung des Gruppenobjekts in Active Directory. Sie können die Anzahl der Tage (Aufbewahrungsdauer) festlegen, bevor die Gruppe gelöscht wird. Eine andere Option ist das Löschen der deprovisionierten Gruppen (sofortiges Verschieben in den Active Directory-Papierkorb). Sie können diese Richtlinie auch so konfigurieren, dass deprovisionierte Gruppen nicht automatisch gelöscht werden.
Benachrichtigungs-verteilung	Im Verlauf eines Deprovisionsvorgangs sendet diese Richtlinie eine Benachrichtigungs-meldung an die angegebenen E-Mail-Empfänger. Sie können den Betreff und den Text der Nachricht anpassen.
Berichtsverteilung	Nach Abschluss eines Deprovisionsvorgangs sendet diese Richtlinie einen Bericht an die angegebenen E-Mail-Empfänger. Der Bericht umfasst eine Liste der während des Deprovisionsvorgangs durchgeführten Aktionen sowie die Details der Deprovisionierungsaktivität. Sie können den Betreff der E-Mail-Nachricht mit dem Bericht anpassen. Sie können die Richtlinie ebenfalls so konfigurieren, dass der Bericht nur dann gesendet wird, wenn im Verlauf eines Deprovisionsvorgangs Fehler aufgetreten sind.
Skriptausführung	Im Verlauf des Deprovisionsvorgangs führt diese Richtlinie das von Ihnen angegebene Skript aus. Mithilfe eines Skripts können Sie benutzerdefinierte Aktionen für die Deprovisionierung implementieren.

Funktionsweise von Richtlinienobjekten

Ein Richtlinienobjekt ist eine Sammlung administrativer Richtlinien, mit denen die durchzusetzenden Geschäftsregeln angegeben werden. Ein Richtlinienobjekt schließt gespeicherte Richtlinienprozeduren und Angaben von Ereignissen ein, die die jeweilige Prozedur aktivieren.

Ein Richtlinienobjekt ordnet seinen Richtlinienprozeduren spezifische Ereignisse zu, bei denen es sich um integrierte Prozeduren oder benutzerdefinierte Skripts handeln kann. Dies ermöglicht das einfache Definieren von Richtlinieneinschränkungen, das Implementieren komplexer Überprüfungskriterien, das Synchronisieren verschiedener Datenquellen und das Ausführen einer Reihe von Verwaltungstasks in einem einzelnen Batch.

ActiveRoles Server setzt Geschäftsregeln durch Verknüpfen von Richtlinienobjekten mit Folgendem um:

- Administrative Ansichten (verwaltete Einheiten von ActiveRoles Server)
- Active Directory-Container (Organisationseinheiten)
- Einzelne Verzeichnisobjekte (Blattobjekte), z.B. Benutzer- oder Gruppenobjekte

Indem Sie auswählen, wo ein Richtlinienobjekt verknüpft wird, bestimmen Sie den Gültigkeitsbereich der Richtlinie. Wenn Sie ein Richtlinienobjekt beispielsweise mit einem Container verknüpfen, unterliegen alle Objekte in dem Container und in seinen Untercontainern normalerweise dem Richtlinienobjekt.

Sie können unterschiedliche Richtlinienobjekte mit unterschiedlichen Containern verknüpfen, um containerspezifische Richtlinien einzurichten. Dies müssen Sie möglicherweise in Situationen ausführen, in denen für jede Organisationseinheit ein eigener Exchange-Server zum Speichern von Postfächern oder ein eigener Dateiserver zum Speichern von Stammordnern verwendet wird.

Sie können ein Richtlinienobjekt auch mit einem Blattobjekt verknüpfen, z.B. mit einem Benutzerobjekt. Betrachten Sie beispielsweise eine Richtlinie, die Änderungen an Gruppenmitgliedschaften beim Kopieren eines bestimmten Benutzerobjekts verbietet.

Richtlinienobjekte definieren das Verhalten des Systems bei der Erstellung, Änderung, Verschiebung oder Löschung von Verzeichnisobjekten im Gültigkeitsbereich der Richtlinie. Richtlinien werden ungeachtet der Administratorrechte des Benutzers durchgesetzt, der die Verwaltungsaufgabe ausführt. Beachten Sie, dass aktive administrative Richtlinien auch für Benutzer mit Administratorrechten für ActiveRoles Server selbst durchgesetzt werden.

Verwaltungsaufgaben für Richtlinienobjekte

In diesem Abschnitt wird die Verwaltung von Richtlinienobjekten mit der ActiveRoles Server-Konsole vorgestellt. Die folgenden Themen werden behandelt:

- Erstellen eines Richtlinienobjekts
- Hinzufügen, Ändern und Entfernen von Richtlinien
- Anwenden von Richtlinienobjekten
- Verwalten des Richtlinienbereichs
- Kopieren eines Richtlinienobjekts
- Exportieren und Importieren von Richtlinienobjekten
- Umbenennen eines Richtlinienobjekts
- Löschen eines Richtlinienobjekts

Erstellen eines Richtlinienobjekts

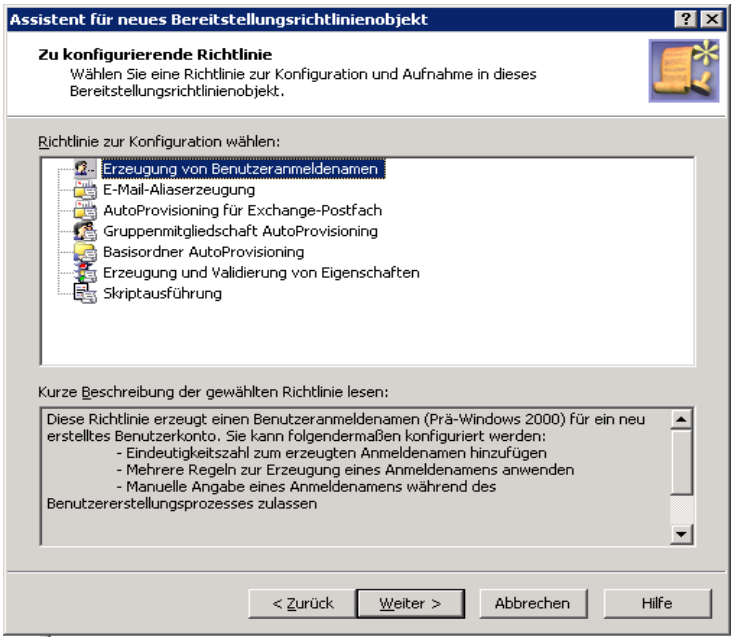
Die ActiveRoles Server-Konsole stellt separate Assistenten für die Erstellung von Richtlinienobjekten in jeder Kategorie (Bereitstellung und Deprovision) bereit. Sie können die Assistenten vom Container **Administration** aus starten. Dieser befindet sich in der Konsolenstruktur unter **Configuration/Policies**:

- Klicken Sie zum Konfigurieren von Bereitstellungsrichtlinien in der Konsolenstruktur mit der rechten Maustaste auf **Verwaltung** und wählen Sie dann **Neu | Richtlinie wird bereitgestellt** aus.
- Klicken Sie zum Konfigurieren von Deprovisionierungsrichtlinien in der Konsolenstruktur mit der rechten Maustaste auf **Verwaltung** und wählen Sie dann **Neu | Deprovisionierungs-richtlinie** aus.

Für die Verwaltung einer großen Anzahl von Richtlinienobjekten sollten Sie wie folgt Container erstellen, die nur angegebene Richtlinienobjekte enthalten, damit Sie sie leicht finden können: Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf **Administration** und wählen Sie dann **Neu | Container**. Verwenden Sie dann die Assistenten, um Richtlinienobjekte in diesem Container zu erstellen: Klicken Sie mit der rechten Maustaste auf den Container, und klicken Sie dann auf **Neu | Bereitstellungsrichtlinie** oder **Neu | Deprovisionierungsrichtlinie**.

Klicken Sie auf der Seite **Willkommen** des Assistenten auf **Weiter**. Geben Sie dann auf der Seite **Name und Beschreibung** einen Namen und eine Beschreibung für das neue Richtlinienobjekt ein. Auf der ActiveRoles Server-Konsole werden im Bereich „Details" in der Liste der Richtlinienobjekte der Name und die Beschreibung angezeigt.

Klicken Sie auf **Weiter**, um den Vorgang fortzusetzen. Nun wird eine Seite angezeigt, auf der Sie die zu konfigurierende Richtlinie auswählen können. Die Liste der Richtlinien hängt davon ab, ob Sie ein Richtlinienobjekt für die Bereitstellung oder eines für die Deprovision erstellen. Beispielsweise ähnelt die Liste der Bereitstellungsrichtlinien der folgenden Abbildung.


Assistent für neues Bereitstellungsrichtlinienobjekt
Zu konfigurierende Richtlinie
Wählen Sie eine Richtlinie zur Konfiguration und Aufnahme in dieses Bereitstellungsrichtlinienobjekt.
Richtlinie zur Konfiguration wählen:
Erzeugung von Benutzeranmeldenamen
E-Mail-Aliaserzeugung
AutoProvisioning für Exchange-Postfach
Gruppenmitgliedschaft AutoProvisioning
Basisordner AutoProvisioning
Erzeugung und Validierung von Eigenschaften
Skriptausführung
Kurze Beschreibung der gewählten Richtlinie lesen:
Diese Richtlinie erzeugt einen Benutzeranmeldenamen (Prä-Windows 2000) für ein neu erstelltes Benutzerkonto. Sie kann folgendermaßen konfiguriert werden:
- Eindeutigkeitszahl zum erzeugten Anmeldenamen hinzufügen
- Mehrere Regeln zur Erzeugung eines Anmeldenamens anwenden
- Manuelle Angabe eines Anmeldenamens während des Benutzererstellungsprozesses zulassen
< Zurück
Weiter >
Abbrechen
Hilfe

Wählen Sie auf der Seite **Zu konfigurierende Richtlinie** den Typ der Richtlinie aus, die Sie dem Richtlinienobjekt hinzufügen möchten. Nach Auswahl des Typs wird seine Beschreibung im unteren Feld angezeigt.

Klicken Sie auf **Weiter**, um die Richtlinie zu konfigurieren. Die Schritte für das Konfigurieren einer Richtlinie hängen vom Richtlinientyp ab. Anweisungen bezüglich der Konfiguration von Richtlinien finden Sie unter „Konfigurationsaufgaben für Richtlinien" weiter unten in diesem Kapitel.

Nach Abschluss der Richtlinienkonfiguration wird eine Seite des Assistenten angezeigt, auf der Sie den Gültigkeitsbereich der Richtlinie angeben können: Sie können eine Liste der Container oder verwalteten Einheiten zusammenstellen, für die die Richtlinie durchgesetzt werden soll. Dieser Schritt ist optional, da Sie den Richtlinienbereich nach der Erstellung des Richtlinienobjekts konfigurieren können (siehe „Anwenden von Richtlinienobjekten" weiter unten in diesem Kapitel).

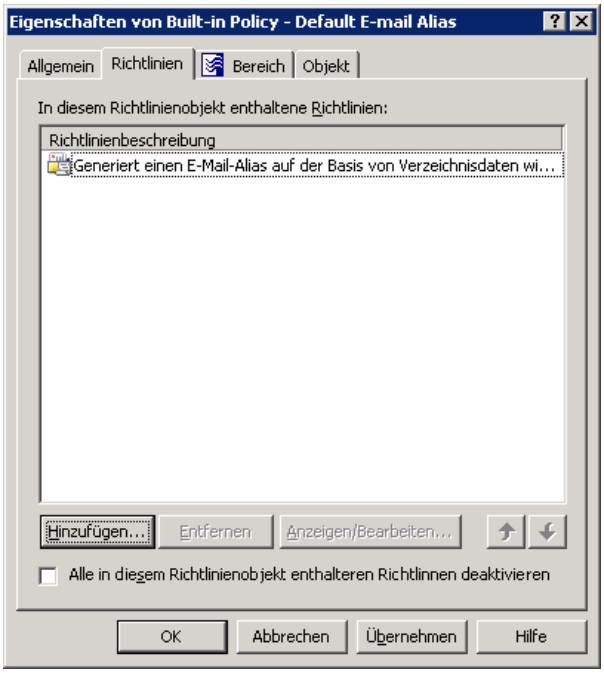
Klicken Sie auf **Weiter**, und klicken Sie dann auf **Fertig stellen**, um den Assistenten abzuschließen. Nun wird das neue Richtlinienobjekt erstellt.

Schrittweise Anleitungen bezüglich der Erstellung eines Richtlinienobjekts finden Sie unter **Anleitungen/Verwalten von Richtlinienobjekten/Erstellen eines Richtlinienobjekts** in der ActiveRoles Server-Hilfe.

Hinzufügen, Ändern und Entfernen von Richtlinien

Mit dem Assistenten „Neues Richtlinienobjekt" kann nur eine Richtlinie konfiguriert werden. Ein Richtlinienobjekt kann jedoch mehrere Richtlinien enthalten. Sie können bei einem vorhandenen Richtlinienobjekt Richtlinien hinzufügen, entfernen oder ihre Optionen ändern, indem Sie seine Eigenschaften wie folgt verwalten: Klicken Sie mit der rechten Maustaste auf das Richtlinienobjekt, und klicken Sie dann auf **Eigenschaften**.

Um Richtlinien in einem Richtlinienobjekt hinzuzufügen, zu entfernen oder zu bearbeiten, verwenden Sie im Dialogfeld **Eigenschaften** die Registerkarte **Richtlinien**. Die Registerkarte ähnelt der folgenden Abbildung:



Auf der Registerkarte **Richtlinien** wird eine Liste der im Richtlinienobjekt definierten Richtlinien angezeigt. Jeder Listeneintrag enthält ein Symbol, das den Typ der Richtlinie angibt, sowie eine Beschreibung der Richtlinie. Die Richtlinien werden in der Reihenfolge ausgeführt, die in der Liste gezeigt wird. Zum Ändern der Reihenfolge können Sie unten rechts auf der Registerkarte die Reihenfolgeschaltflächen mit den Pfeilen verwenden.

Auf der Registerkarte **Richtlinien** können Sie folgende Verwaltungsaufgaben ausführen:

- **Richtlinie hinzufügen** Klicken Sie auf die Schaltfläche **Hinzufügen** und folgen Sie den Anweisungen des Assistenten. Diese hängen davon ab, ob Sie ein Richtlinienobjekt für die Bereitstellung oder eines für die Deprovision konfigurieren.

  Der Assistent fordert Sie auf, den Typ der hinzuzufügenden Richtlinie auszuwählen, und führt Sie dann durch die Schritte zum Konfigurieren der Richtlinie. Die Schritte für das Konfigurieren einer Richtlinie hängen vom Richtlinientyp ab. Anweisungen bezüglich der Konfiguration von Richtlinien finden Sie unter „Konfigurationsaufgaben für Richtlinien" weiter unten in diesem Kapitel.

- **Richtlinie löschen** Wählen Sie in der Liste Richtlinien aus, und klicken Sie auf die Schaltfläche **Entfernen**. So werden die ausgewählten Richtlinien permanent gelöscht.
- **Richtlinie ändern** Wählen Sie in der Liste eine Richtlinie aus und klicken Sie auf die Schaltfläche **Anzeigen/Bearbeiten**. Nun wird das Dialogfeld **Eigenschaften** für die ausgewählte Richtlinie angezeigt.

  Das Dialogfeld **Eigenschaften** enthält mehrere Registerkarten. Jede Registerkarte enthält die gleichen Optionen wie die entsprechende Seite des Assistenten, mit dem die Richtlinie konfiguriert wird. Sie können Richtlinienoptionen hier genauso verwalten wie beim anfänglichen Konfigurationsvorgang.

- **Alle Richtlinien deaktivieren** Für die Problembehandlung müssen Sie möglicherweise die Durchsetzung der Richtlinien beenden, ohne sie zu löschen. Aktivieren Sie dazu das Kontrollkästchen **Alle in diesem Richtlinienobjekt enthaltenen Richtlinien deaktivieren**.

Welche Richtlinien einem bestimmten Richtlinienobjekt hinzugefügt werden können, hängt vom Typ des Richtlinienobjekts ab. Ein Bereitstellungsrichtlinienobjekt kann nur bereitstellungsrelevante Richtlinien enthalten, während ein Deprovisionsrichtlinienobjekt nur deprovisionsrelevante Richtlinien enthalten kann (siehe „Bereitstellungsrichtlinienobjekte" und „Richtlinienobjekte zur Bereitstellungsrücknahme" weiter oben in diesem Kapitel).

Schrittweise Anleitungen bezüglich des Hinzufügens, Bearbeitens oder Entfernens von Richtlinien zu/in/aus einem Richtlinienobjekt finden Sie in den Themen **Hinzufügen von Richtlinien zu einem Richtlinienobjekt**, **Ändern von Richtlinien in einem Richtlinienobjekt** und **Entfernen von Richtlinien aus einem Richtlinienobjekt** unter der Überschrift **Anleitungen/Verwalten von Richtlinienobjekten** in der ActiveRoles Server-Hilfe.

Anwenden von Richtlinienobjekten

Das Implementieren einer Richtlinie für die Durchsetzung von Geschäftsregeln umfasst zwei Phasen. Das Konfigurieren der Richtlinie in einem Richtlinienobjekt ist nur der erste Schritt. Beim Erstellen einer neuen Richtlinie wählen Sie aus den verfügbaren Optionen einen Richtlinientyp aus und definieren dann die Optionen, aus denen die Richtlinie besteht. Der zweite Schritt besteht darin, mit Hilfe der ActiveRoles Server-Konsole die Richtlinie für die gewünschten Verzeichnisbereiche durchzusetzen.

Mit ActiveRoles Server können Richtlinien für ein beliebiges Verzeichnisobjekt durchgesetzt werden, d.h. für eine administrative Ansicht (verwaltete Einheit), einen Verzeichnisordner (Container) oder ein einzelnes Objekt (Blattobjekt). Richtlinien werden durchgesetzt, indem ein Richtlinienobjekt angewendet (verknüpft) wird, das sie enthält.

Wenn Sie ein Richtlinienobjekt auf eine verwaltete Einheit oder einen Verzeichnisordner anwenden, steuern die Richtlinien die Objekte in dieser Einheit oder diesem Ordner sowie auch die Einheit oder den Ordner selbst. Wenn Sie ein Richtlinienobjekt auf ein Blattobjekt anwenden, wie etwa auf einen Benutzer oder eine Gruppe, steuern die Richtlinien nur dieses Objekt. Wenn Sie beispielsweise ein Richtlinienobjekt auf eine Gruppe anwenden, hat dies keine Auswirkungen auf die Mitglieder der Gruppe.

Die Objekte, die einem gegebenen Richtlinienobjekt unterliegen, die also von den in diesem Richtlinienobjekt definierten Richtlinien gesteuert werden, werden als sein *Richtlinienbereich* bezeichnet. Wenn Sie beispielsweise ein Richtlinienobjekt auf eine verwaltete Einheit anwenden, besteht der Richtlinienbereich aus den Objekten innerhalb dieser verwalteten Einheit.

Der Richtlinienbereich enthält also normalerweise alle Objekte in einem Container oder einer verwalteten Einheit, auf den bzw. auf die das Richtlinienobjekt angewendet wird. Manchmal müssen jedoch einzelne Objekte oder Untercontainer aus dem Richtlinienbereich ausgeschlossen werden, damit sich die Richtlinien auf bestimmte Objekte nicht auswirken.

Mit ActiveRoles Server können Sie Objekte oder gesamte Container selektiv aus dem Richtlinienbereich ausschließen. Sie können die Vererbung von Richtlinien für einzelne Objekte oder Container blockieren und so den Richtlinienbereich verfeinern. Die Option zum sperren der Richtlinienvererbung wird weiter unten in diesem Abschnitt beschrieben (siehe „Verwalten des Richtlinienbereichs" weiter unten in diesem Kapitel).

Um ein Richtlinienobjekt anzuwenden, können Sie von einem beliebigen der folgenden Punkte aus starten:

- **Richtlinienobjekt** Fügen Sie dem Richtlinienbereich des Richtlinienobjekts verwaltete Einheiten oder Container hinzu.
- **Verzeichnisobjekt** Fügen Sie das Richtlinienobjekt der Richtlinienliste für das Verzeichnisobjekt hinzu.

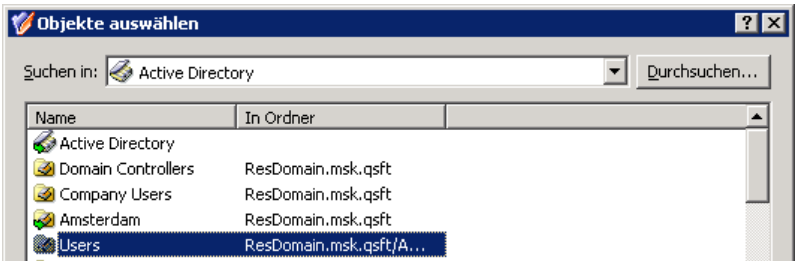
In den folgenden zwei Abschnitten werden diese Optionen ausführlich beschrieben. Schrittweise Anleitungen bezüglich der Anwendung eines Richtlinienobjekts finden Sie unter **Anleitungen/Verwalten von Richtlinienobjekten/Anwenden eines Richtlinienobjekts** in der ActiveRoles Server-Hilfe.

Hinzufügen von verwalteten Einheiten oder Containern zu einem Richtlinienbereich

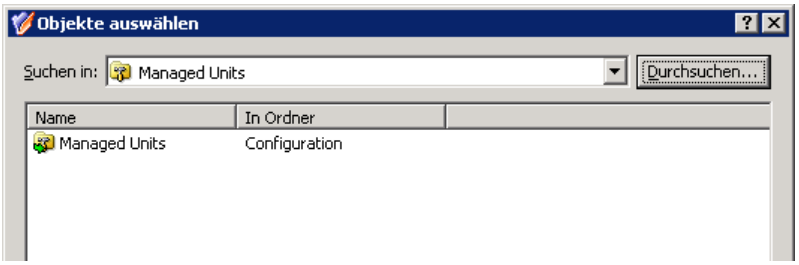
Sie können administrative Ansichten (verwaltete Einheiten) sowie Verzeichnisordner (Container) auf folgende Weisen zum Richtlinienbereich eines bestimmten Richtlinienobjekts hinzufügen:

- Klicken Sie mit der rechten Maustaste auf das Richtlinienobjekt, und klicken Sie dann auf **Richtlinienbereich**. Klicken Sie anschließend im Fenster **ActiveRoles Serverrichtlinien-bereich** auf die Schaltfläche **Hinzufügen**.
- Stellen Sie sicher, dass im Menü **Ansicht** die Option **Erweiterte Detailansicht** aktiviert ist. Wählen Sie dann das Richtlinienobjekt aus. Klicken Sie im Bereich „Details" auf der Registerkarte **ActiveRoles Serverrichtlinienbereich** mit der rechten Maustaste in einen leeren Bereich, und klicken Sie dann auf **Hinzufügen**.

In beiden Fällen wird durch Klicken auf **Hinzufügen** das Fenster **Objekte auswählen** angezeigt, in dem Sie Container und verwaltete Einheiten auswählen können. Um eine Liste auswählbarer Container zu erstellen, klicken Sie auf die Schaltfläche **Durchsuchen**, und wählen Sie **Active Directory** oder einen Container in der Hierarchie unter **Active Directory** aus. Die Liste ähnelt der folgenden Abbildung:



Um eine Liste auswählbarer verwalteter Einheiten zu erstellen, klicken Sie auf die Schaltfläche **Durchsuchen** und wählen Sie **Managed Units** oder einen Container in der Hierarchie unter **Managed Units** aus. Die Liste ähnelt der folgenden Abbildung:



Wählen Sie im Fenster **Objekte auswählen** in der Liste Container oder verwaltete Einheiten aus, und klicken Sie auf die Schaltfläche **Hinzufügen**, um die entstehende Elementliste zu erstellen. Klicken Sie abschließend auf **OK**.

Hinzufügen von Richtlinienobjekten zu Richtlinienlisten für ein Verzeichnisobjekt

Für ein gegebenes Verzeichnisobjekt (Container, Benutzer, Gruppe usw.) wird eine Liste von Richtlinienobjekten, die sich auf das Verzeichnisobjekt auswirken, als *Richtlinienliste* bezeichnet. Wenn das Verzeichnisobjekt sich im Verzeichnisbereich eines gegebenen Richtlinienobjekts befindet, ist das Richtlinienobjekt in die Richtlinienliste dieses Verzeichnisobjekts eingeschlossen.

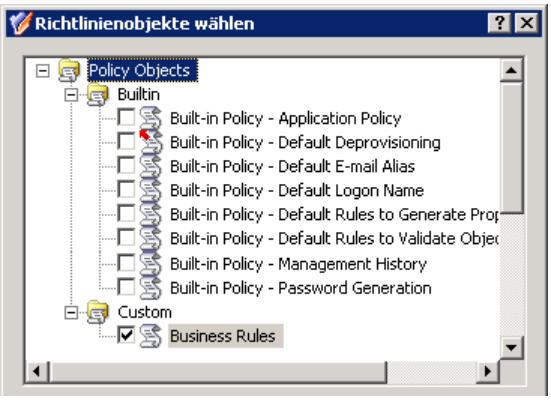
Die Schritte zum Hinzufügen eines Richtlinienobjekts zur Richtlinienliste für ein Verzeichnisobjekt hängen davon ab, ob es ein Container oder ein Blattobjekt ist:

- Klicken Sie mit der rechten Maustaste auf eine verwaltete Einheit oder einen Container und dann auf **Richtlinie erzwingen**. Klicken Sie anschließend im Fenster **ActiveRoles Serverrichtlinie** auf die Schaltfläche **Hinzufügen**.
- Klicken Sie mit der rechten Maustaste auf ein Blattobjekt (Benutzer, Gruppe o.ä.) und dann auf **Eigenschaften**, öffnen Sie die Registerkarte **Verwaltung** und klicken Sie auf die Schaltfläche **Richtlinie**. Klicken Sie anschließend im Fenster **ActiveRoles Serverrichtlinie** auf die Schaltfläche **Hinzufügen**.

Wenn Sie das erweiterte Detailfenster verwenden (d.h. wenn im Menü **Ansicht** die Option **Erweiterte Detailansicht** aktiviert ist), können Sie dies unabhängig vom Typ des Verzeichnisobjekts wie folgt erreichen:

- Wählen Sie das Verzeichnisobjekt aus, öffnen Sie im Bereich „Details" die Registerkarte **AR-Serverrichtlinie**, klicken Sie mit der rechten Maustaste in einen leeren Bereich auf der Registerkarte, und klicken Sie dann auf **Hinzufügen**.

In allen Fällen wird durch Klicken auf **Hinzufügen** das Fenster **Richtlinienobjekte wählen** angezeigt, in dem Sie hinzuzufügende Richtlinienobjekte auswählen können. Aktivieren Sie die Kontrollkästchen neben den Namen von Richtlinienobjekten, wie in der folgenden Abbildung gezeigt, und klicken Sie dann auf **OK**.


Richtlinienobjekte wählen
Policy Objects
Builtin
Built-in Policy - Application Policy
Built-in Policy - Default Deprovisioning
Built-in Policy - Default E-mail Alias
Built-in Policy - Default Logon Name
Built-in Policy - Default Rules to Generate Prop
Built-in Policy - Default Rules to Validate Objec
Built-in Policy - Management History
Built-in Policy - Password Generation
Custom
Business Rules

Verwalten des Richtlinienbereichs

Beim Anwenden eines Richtlinienobjekts auf ein Verzeichnisobjekt erstellt ActiveRoles Server eine Richtlinienobjektverknüpfung. Richtlinien werden also durch Verknüpfen von Richtlinienobjekten mit Verzeichnisobjekten aktiviert, d.h. mit verwalteten Einheiten, Verzeichnisordnern (Containern) oder einzelnen Objekten (Blattobjekten).

Jede Richtlinienobjektverknüpfung enthält die folgenden Informationen:

- Das Richtlinienobjekt, das die Richtlinien definiert
- Das Verzeichnisobjekt, das Ziel der Verknüpfung ist
- Das Flag (Einschließen oder Ausschließen), das angibt, ob das Verzeichnisobjekt in den Richtlinienbereich eingeschlossen wird

Sie können über eine der folgenden Möglichkeiten eine Liste von Richtlinienobjekten anzeigen:

- **Richtlinienobjekt** Klicken Sie mit der rechten Maustaste auf ein Richtlinienobjekt und klicken Sie dann auf **Richtlinienbereich**.

  Dies zeigt die Verknüpfungen an, in denen das Richtlinienobjekt auftritt.

- **Verzeichnisobjekt** Öffnen Sie zunächst wie folgt ein Fenster mit einer Liste der Richtlinienobjekte, die sich auf dieses Verzeichnisobjekt auswirken:
  - Auf ein Containerobjekt oder eine verwaltete Einheit klicken Sie mit der rechten Maustaste, und klicken Sie dann auf **Richtlinie erzwingen**.
  - Für ein Blattobjekt öffnen Sie das Dialogfeld **Eigenschaften**, öffnen die Registerkarte **Verwaltung** und klicken auf **Richtlinie**.

  Im nun geöffneten Fenster klicken Sie auf die Schaltfläche **Erweitert**.

  Damit werden die Verknüpfungen angezeigt, in denen das Verzeichnisobjekt als Zielobjekt auftritt.

Sie können eine Liste von Richtlinienobjektverknüpfungen auch über das erweiterte Detailfenster anzeigen. Stellen Sie sicher, dass im Menü **Ansicht** die Option **Erweiterte Detailansicht** aktiviert ist, und führen Sie dann eine der folgenden Aktionen aus:

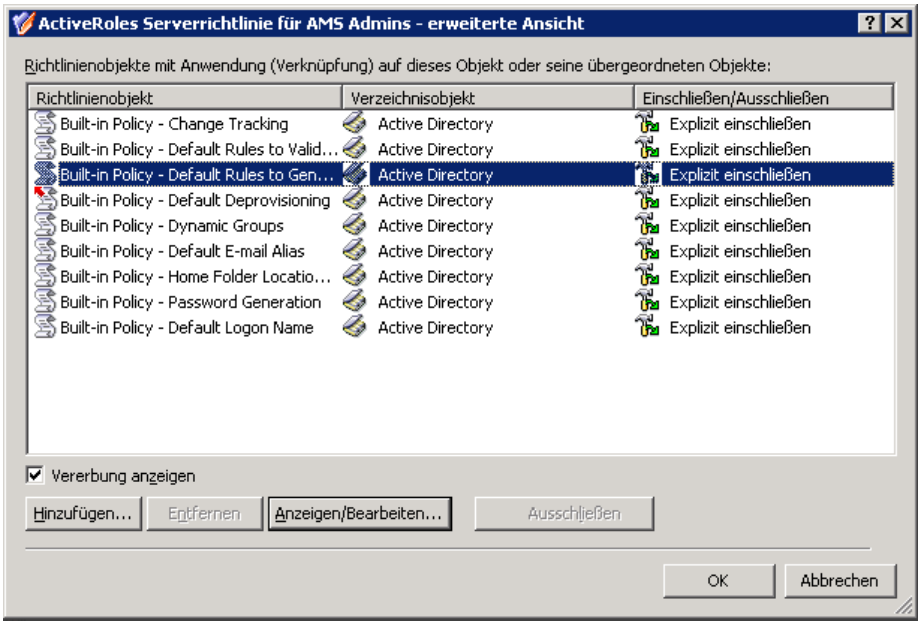
- Wählen Sie ein Richtlinienobjekt aus.

  Auf der Registerkarte **ActiveRoles Serverrichtlinienbereich** werden die Verknüpfungen aufgelistet, in denen das ausgewählte Richtlinienobjekt auftritt.

- Wählen Sie ein Verzeichnisobjekt (verwaltete Einheit, Container oder Blattobjekt) aus, klicken Sie mit der rechten Maustaste in einen leeren Bereich auf der Registerkarte **AR-Serverrichtlinie**, und klicken Sie dann auf **Erweiterte Ansicht**.

  Damit werden die Verknüpfungen angezeigt, in denen das Verzeichnisobjekt als Zielobjekt auftritt.

Wenn Sie eine Liste von Richtlinienobjektverknüpfungen für ein Verzeichnisobjekt anzeigen, wird die Liste in einem Fenster angezeigt, das der folgenden Abbildung ähnelt.



Jeder Eintrag in der Liste schließt die folgenden Informationen ein:

- **Richtlinienobjekt** Name des Richtlinienobjekts.
- **Verzeichnisobjekt** Kanonischer Name des Objekts, mit dem das Richtlinienobjekt verknüpft ist, d.h. des Zielobjekts der Verknüpfung.
- **Einschließen/Ausschließen** Flag, das das Verhalten der Verknüpfung bestimmt:
  - **Explizit einschließen** bedeutet, dass die Verknüpfung das Zielobjekt in den Richtlinienbereich aufnimmt, d.h. dass die im Richtlinienobjekt definierten Richtlinien das Zielobjekt steuern.
  - **Explizit ausschließen** bedeutet, dass die Verknüpfung das Zielobjekt nicht in den Richtlinienbereich aufnimmt, d.h. dass die im Richtlinienobjekt definierten Richtlinien das Zielobjekt nicht steuern.

  Das Flag **Ausschließen** hat Vorrang vor dem Flag **Einschließen**. Wenn zwei Verknüpfungen mit demselben Richtlinienobjekt vorhanden sind, von denen eine das Flag **Einschließen** und die andere das Flag **Ausschließen** aufweist, wird das Objekt aus dem Richtlinienbereich des Richtlinienobjekts ausgeschlossen.

In der Liste der Richtlinienobjektverknüpfungen werden die Verknüpfungen der folgenden Kategorien angezeigt:

- **Direkte Verknüpfungen** Das Richtlinienobjekt wird direkt auf das ausgewählte Objekt angewendet (mit ihm verknüpft).
- **Geerbte Verknüpfungen** Das Richtlinienobjekt wird auf einen Container in der Containerhierarchie über dem ausgewählten Objekt oder auf eine verwaltete Einheit, zu der das ausgewählte Objekt gehört, angewendet (mit ihm/ihr verknüpft).

Die von übergeordneten Objekte geerbten Verknüpfungen können aus der Liste herausgefiltert werden. Deaktivieren Sie hierzu das Kontrollkästchen **Vererbung anzeigen**.

Zum Verwalten von Verknüpfungen können Sie die Schaltflächen unter der Liste verwenden:

- **Hinzufügen** Zeigt das Dialogfeld an, in dem Sie Richtlinienobjekte auswählen können, um Verknüpfungen zu ihnen zu erstellen.
- **Entfernen** Löscht die ausgewählten Einträge aus der Verknüpfungsliste. Nur für direkte Verknüpfungen verfügbar.
- **Anzeigen/Bearbeiten** Zeigt das Dialogfeld zum Anzeigen oder Ändern von Verknüpfungseigenschaften an (z.B. der Eigenschaft), die angibt, ob die Verknüpfung sich auf die untergeordneten Objekten ihres Zielobjekts auswirkt. Nur für die Verknüpfungen mit dem Flag **Einschließen** verfügbar.
- **Ausschließen** Wird für Verknüpfungen mit dem Flag **Einschließen** angezeigt. Nur für direkte Verknüpfungen verfügbar. Ändert das Flag auf **Ausschließen**.
- **Einschließen** Wird für Verknüpfungen mit dem Flag **Ausschließen** angezeigt. Nur für direkte Verknüpfungen verfügbar. Ändert das Flag auf **Einschließen**.

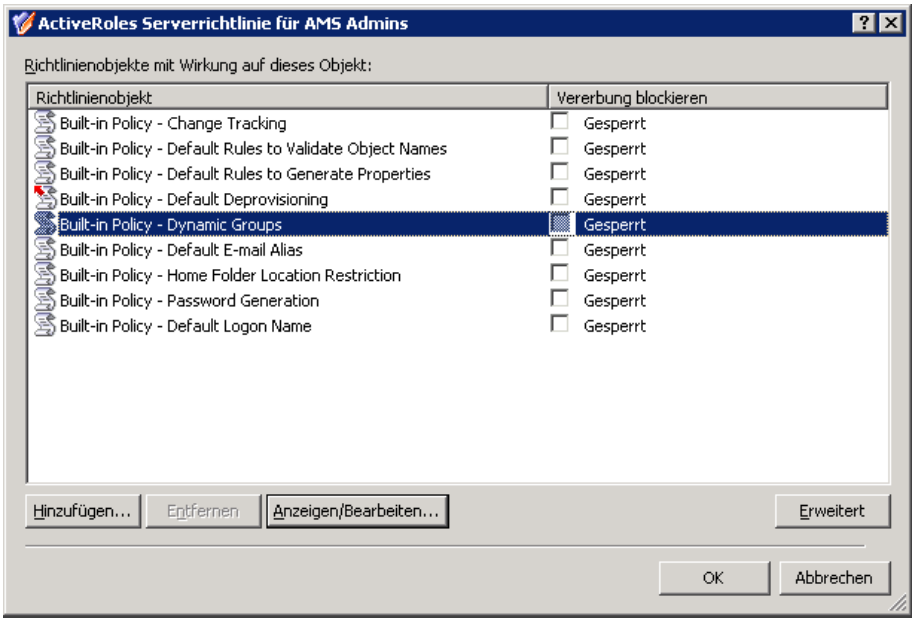
Die Schaltfläche **Entfernen** ist nur für direkte Verknüpfungen verfügbar. Wenn Sie Verknüpfungen löschen möchten, sollten Sie sie mit dem Befehl **Richtlinienbereich** für das Richtlinienobjekt verwalten.

Um die Verwaltung der Auswirkungen von Richtlinien auf Verzeichnisobjekte zu vereinfachen, ermöglicht Ihnen die ActiveRoles Server-Konsole das Verwalten des Richtlinienbereichs ohne direktes Verwalten von Verknüpfungen mit Richtlinienobjekten. Die Richtlinienliste eines Verzeichnisobjekts ist eine Liste der Richtlinienobjekte, die das Verzeichnisobjekt steuern, d.h. sich auf es auswirken. Sie können diese Richtlinienliste anzeigen und ändern, statt durch direkte und indirekte Verknüpfungen navigieren zu müssen.

Sie können die Richtlinienliste eines gegebenen Verzeichnisobjekts wie folgt anzeigen:

- Auf einen Container oder eine verwaltete Einheit klicken Sie mit der rechten Maustaste, und klicken dann auf **Richtlinie erzwingen**.
- Auf ein Blattobjekt (Benutzer, Gruppe o.ä.) klicken Sie mit der rechten Maustaste, klicken Sie dann auf **Eigenschaften**, öffnen Sie die Registerkarte **Verwaltung** und klicken Sie auf die Schaltfläche **Richtlinie**.

Damit wird ein Fenster angezeigt, das der folgenden Abbildung ähnelt.



Jeder Eintrag in der Liste schließt die folgenden Informationen ein:

- **Richtlinienobjekt** Der Name des Richtlinienobjekts. Das Richtlinienobjekt steuert dieses Verzeichnisobjekt aufgrund einer direkten Verknüpfung oder geerbter Verknüpfungen.
- **Vererbung blockieren** Zeigt an, ob die Auswirkung der Richtlinie für dieses Verzeichnisobjekt blockiert ist. Wenn das Kontrollkästchen **Gesperrt** aktiviert ist, wird die Richtlinienobjektverknüpfung mit dem Flag **Ausschließen** für dieses Verzeichnisobjekt erstellt.

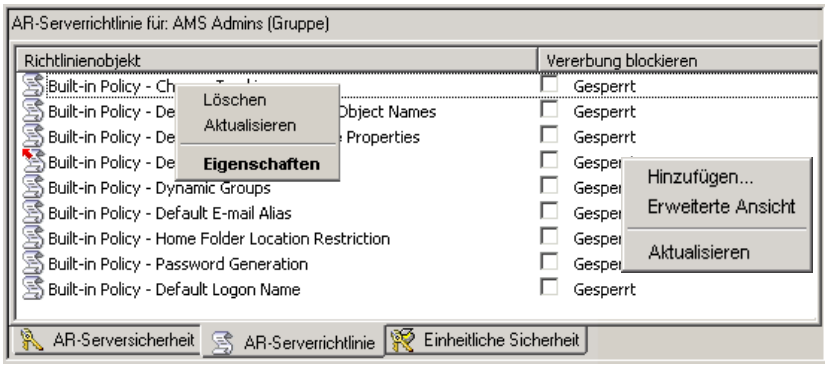
Sie können die Richtlinienliste mit Hilfe der Schaltflächen unter der Liste verwalten:

- **Hinzufügen** Zeigt das Dialogfeld an, in dem Sie Richtlinienobjekte auswählen können, um das Verzeichnisobjekt ihrer Steuerung zu unterstellen.
- **Entfernen** Wenn Sie in der Richtlinienliste ein Richtlinienobjekt auswählen und auf **Entfernen** klicken, wird die direkte Verknüpfung des Richtlinienobjekts mit diesem Objekt gelöscht.

  Wenn sich das Richtlinienobjekt aufgrund einer geerbten Verknüpfung in der Liste befindet, ist die Schaltfläche **Entfernen** nicht verfügbar. Wenn außerdem sowohl die direkte Verknüpfung als auch eine geerbte Verknüpfung für das Richtlinienobjekt vorhanden sind, wird durch Klicken auf **Entfernen** die direkte Verknüpfung gelöscht, aber *nicht* das Richtlinienobjekt aus der Richtlinienliste gelöscht. In diesem Fall verbleibt das Richtlinienobjekt in der Liste, weil die Richtlinien aufgrund der Vererbung weiterhin angewendet werden.

  Wenn Sie das Verzeichnisobjekt aus dem Richtlinienbereich eines bestimmten Richtlinienobjekts entfernen möchten, aktivieren Sie das Kontrollkästchen **Gesperrt** in der Spalte **Vererbung blockieren**. Dies fügt die Richtlinienobjektverknüpfung mit dem Flag **Ausschließen** für das Verzeichnisobjekt hinzu.
- **Anzeigen/Bearbeiten** Zeigt das Dialogfeld **Eigenschaften** für das Richtlinienobjekt an, das Sie in der Liste auswählen. Mit dem Dialogfeld **Eigenschaften** können Sie Richtlinien im Richtlinienobjekt verwalten und Zugriff auf die Liste aller Verknüpfungen erhalten, in denen dieses Richtlinienobjekt vorkommt.
- **Erweitert** Öffnet das Fenster mit der Liste der Richtlinienobjektverknüpfungen für dieses Verzeichnisobjekt, die weiter oben in diesem Abschnitt erörtert wird.

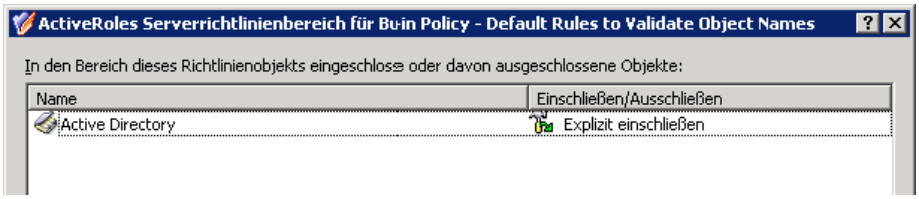
Sie können auf die Richtlinienliste auch über das erweiterte Detailfenster zugreifen. Die Liste wird auf der Registerkarte **AR-Serverrichtlinie** angezeigt, wenn Sie ein Verzeichnisobjekt auswählen:



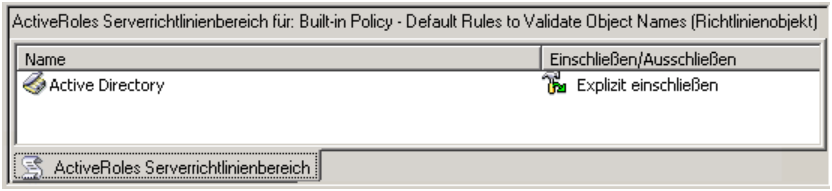
Auf dieser Registerkarte können Sie die die gleichen Verwaltungsaufgaben ausführen wie im Fenster **ActiveRoles Serverrichtlinie**: Klicken Sie mit der rechten Maustaste auf einen Listeneintrag oder in einen leeren Bereich, und verwenden Sie Befehle aus dem Kontextmenü. Die Befehle haben die gleichen Funktionen wie die Schaltflächen im Fenster **ActiveRoles Serverrichtlinie**.

Sie können den Richtlinienbereich eines gegebenen Richtlinienobjekts auch mit Hilfe einer Liste von Verzeichnisobjekten verwalten, auf die das Richtlinienobjekt angewendet wird (mit denen es verknüpft ist). Die Liste kann in einem separaten Fenster oder auf einer Registerkarte im erweiterten Detailfenster angezeigt werden:

- Um die Liste in einem Fenster anzuzeigen, klicken Sie mit der rechten Maustaste auf das Richtlinienobjekt und klicken dann auf **Richtlinienbereich**. Die Liste ähnelt der folgenden Abbildung.


ActiveRoles Serverrichtlinienbereich für Built-in Policy - Default Rules to Validate Object Names
In den Bereich dieses Richtlinienobjekts eingeschlossene oder davon ausgeschlossene Objekte:
Name
Einschließen/Ausschließen
Active Directory
Explizit einschließen

- Um die Liste auf einer Registerkarte anzuzeigen, stellen Sie sicher, dass im Menü **Ansicht** die Option **Erweiterte Detailansicht** aktiviert ist, und wählen Sie das Richtlinienobjekt aus. Die Liste ähnelt der folgenden Abbildung.



In der Liste werden alle Verknüpfungen des Richtlinienobjekts angezeigt. Jeder Eintrag in der Liste schließt die folgenden Informationen ein:

- **Name** Kanonischer Name des Verzeichnisobjekts, mit dem das Richtlinienobjekt verknüpft ist, d.h. des Zielobjekts der Verknüpfung.
- **Einschließen/Ausschließen** Flag, das das Verhalten der Verknüpfung bestimmt:
  - **Explizit einschließen** bedeutet, dass die Verknüpfung das Zielobjekt in den Richtlinienbereich aufnimmt, d.h. dass die im Richtlinienobjekt definierten Richtlinien das Zielobjekt steuern.
  - **Explizit ausschließen** bedeutet, dass die Verknüpfung das Zielobjekt nicht in den Richtlinienbereich aufnimmt, d.h. dass die im Richtlinienobjekt definierten Richtlinien das Zielobjekt nicht steuern.

  Das Flag **Ausschließen** hat Vorrang vor dem Flag **Einschließen**. Wenn zwei Verknüpfungen mit demselben Zielobjekt vorhanden sind, von denen eine das Flag **Einschließen** und die andere das Flag **Ausschließen** aufweist, wird das Zielobjekt aus dem Richtlinienbereich des Richtlinienobjekts ausgeschlossen.

Zum Verwalten der Liste im Fenster **ActiveRoles Serverrichtlinienbereich** können Sie die Schaltflächen unterhalb der Liste verwenden: **Hinzufügen**, **Entfernen**, **Anzeigen/Bearbeiten** und **Einschließen** oder **Ausschließen**. Diese Schaltflächen haben etwa die gleichen Funktionen wie die weiter oben in diesem Abschnitt bei der Erörterung der Verwaltungsaufgaben für Richtlinienobjektverknüpfungen beschriebenen. Zum Verwalten der Liste auf der Registerkarte **ActiveRoles Serverrichtlinienbereich** können Sie die Befehle im Kontextmenü verwenden: Klicken Sie mit der rechten Maustaste auf eine Verknüpfung oder in einen leeren Bereich, um auf das Menü zuzugreifen. Das Menü enthält die folgenden Befehle:

- **Hinzufügen** Wird angezeigt, wenn Sie mit der rechten Maustaste in einen leeren Bereich klicken. Führt die gleiche Aktion aus wie die Schaltfläche **Hinzufügen**. Öffnet das Dialogfeld **Objekte auswählen**, in dem Sie Container oder verwaltete Einheiten auswählen können, mit denen Sie das Richtlinienobjekt verknüpfen möchten (siehe auch „Anwenden von Richtlinienobjekten").
- **Löschen** Wird angezeigt, wenn Sie mit der rechten Maustaste auf eine Verknüpfung klicken. Führt die gleiche Aktion aus wie die Schaltfläche **Entfernen**. Löscht die ausgewählte Verknüpfung aus der Liste.
- **Ausschließen** Wird angezeigt, wenn Sie mit der rechten Maustaste auf eine Verknüpfung mit dem Flag **Einschließen** klicken. Führt die gleiche Aktion aus wie die Schaltfläche **Ausschließen**. Ändert das Flag für die ausgewählte Verknüpfung.
- **Einschließen** Wird angezeigt, wenn Sie mit der rechten Maustaste auf eine Verknüpfung mit dem Flag **Ausschließen** klicken. Führt die gleiche Aktion aus wie die Schaltfläche **Einschließen**. Ändert das Flag für die ausgewählte Verknüpfung.
- **Aktualisieren** Aktualisiert die Liste mit den aktuellen Informationen.

Kopieren eines Richtlinienobjekts

Mit der ActiveRoles Server-Konsole können Sie Kopien von Richtlinienobjekten erstellen. Mit dieser Funktion können Sie vorhandene Richtlinienobjekte wieder verwenden.

Zum Erstellen einer Kopie eines Richtlinienobjekts klicken Sie mit der rechten Maustaste auf das Richtlinienobjekt, und klicken Sie dann auf **Kopieren**. Hierdurch wird der Assistent „Objekt kopieren" geöffnet. Geben Sie einen Namen und eine Beschreibung für die Kopie ein, und klicken Sie dann auf **Weiter**.

Auf der nächsten Seite des Assistenten wird eine Liste von Richtlinien angezeigt. Die Liste enthält alle im ursprünglichen Richtlinienobjekt definierten Richtlinien. Klicken Sie auf **Fertig stellen**, um die Kopie zu erstellen.

Die Kopie besitzt die gleichen Eigenschaften wie das ursprüngliche Richtlinienobjekt, einschließlich der Richtlinien und ihrer Konfigurationen. Im Dialogfeld **Eigenschaften** können Sie Änderungen an der Kopie vornehmen, wie dies weiter oben in diesem Kapitel beschrieben wurde (siehe „Hinzufügen, Ändern und Entfernen von Richtlinien").

Schrittweise Anleitungen bezüglich der Erstellung einer Kopie eines Richtlinienobjekts finden Sie unter **Anleitungen/Verwalten von Richtlinienobjekten/Kopieren eines Richtlinienobjekts** in der ActiveRoles Server-Hilfe.

Exportieren und Importieren von Richtlinienobjekten

Mit der ActiveRoles Server-Konsole können Sie Richtlinienobjekte in eine XML-Datei exportieren und sie dann aus dieser Datei importieren, um eine andere Instanz von ActiveRoles Server aufzufüllen. Die Export- und Importvorgänge stellen eine Möglichkeit bereit, Richtlinienobjekte von einer Testumgebung in eine Produktionsumgebung zu verschieben.

Wenn Sie Richtlinienobjekte erst exportieren und dann importieren, werden nur Richtlinien übertragen. Die Richtlinienobjektverknüpfungen werden in den Export-Import-Vorgang nicht eingeschlossen. Sie müssen sie nach Abschluss des Vorgangs manuell neu konfigurieren.

Um Richtlinienobjekte zu exportieren, wählen Sie sie aus, klicken Sie mit der rechten Maustaste auf die Auswahl und wählen Sie dann **Alle Aufgaben | Exportieren**. Geben Sie im Dialogfeld **Objekte exportieren** die Datei an, in der Sie die Daten speichern möchten, und klicken Sie dann auf **Speichern**.

Zum Importieren von Richtlinienobjekten klicken Sie mit der rechten Maustaste auf den Container, in dem Sie die Richtlinienobjekte ablegen möchten, und klicken Sie dann auf **Importieren**. Wählen Sie im Dialogfeld **Verzeichnisobjekte importieren** die Datei aus, in die die Richtlinienobjekte exportiert wurden, und klicken Sie dann auf **Öffnen**.

Schrittweise Anleitungen bezüglich des Exports und Imports von Richtlinienobjekten finden Sie in den Themen **Exportieren eines Richtlinienobjekts** und **Importieren eines Richtlinienobjekts** unter **Anleitungen/Verwalten von Richtlinienobjekte** in der ActiveRoles Server-Hilfe.

Umbenennen eines Richtlinienobjekts

Zum Umbenennen eines Richtlinienobjekts klicken Sie mit der rechten Maustaste auf das Richtlinienobjekt, und klicken Sie dann auf **Umbenennen**. Geben Sie den neuen Namen ein, und drücken Sie dann die Eingabetaste. Das Umbenennen eines Richtlinienobjekts hat keine Auswirkungen auf seine Verknüpfungen. Der Grund ist, dass auf Richtlinienobjekte über unveränderliche Bezeichner statt über ihre Namen verwiesen wird.

Schrittweise Anleitungen finden Sie unter **Anleitungen/Verwalten von Richtlinienobjekten/ Umbenennen eines Richtlinienobjekts** in der ActiveRoles Server-Hilfe.

Löschen eines Richtlinienobjekts

Um ein Richtlinienobjekt zu löschen, müssen Sie zunächst die Verknüpfungen mit dem Richtlinienobjekt löschen (siehe „Verwalten des Richtlinienbereichs“ weiter oben in diesem Kapitel). Dann können Sie den Löschvorgang wie folgt ausführen: Klicken Sie mit der rechten Maustaste auf das Richtlinienobjekt, und klicken Sie dann auf **Löschen**.

Schrittweise Anleitungen finden Sie unter **Anleitungen/Verwalten von Richtlinienobjekten/ Löschen eines Richtlinienobjekts** in der ActiveRoles Server-Hilfe.

Konfigurationsaufgaben für Richtlinien

In diesem Abschnitt wird beschrieben, wie Sie Richtlinien der folgenden Typen konfigurieren können, gruppiert nach Richtlinienobjektkategorie:

RICHTLINIENOBJEKTKATEGORIE	RICHTLINIENTYP
Bereitstellungsrichtlinienobjekt	Erzeugung und Validierung von Eigenschaften
	Erzeugung von Benutzeranmeldenamen
	Automatische Bereitstellung der Gruppenmitgliedschaft
	E-Mail-Aliaserzeugung
	Automatische Bereitstellung von Exchange-Postfächern
	Automatische Bereitstellung des Stammordners
	Skriptausführung
Deprovisionsrichtlinienobjekt	Benutzerkontodeprovisionierung
	Entfernen der Gruppenmitgliedschaft
	Deprovisionierung des Exchange-Postfachs
	Stammordner-Deprovisionierung
	Benutzerkonto-Verschiebung
	Permanentes Löschen von Benutzerkonten
	Gruppenobjekt-Deprovisionierung
	Gruppenobjekt-Verschiebung
	Dauerhaftes Löschen des Gruppenobjekts
	Benachrichtigungsverteilung
	Berichtsverteilung
	Skriptausführung

Erzeugung und Validierung von Eigenschaften

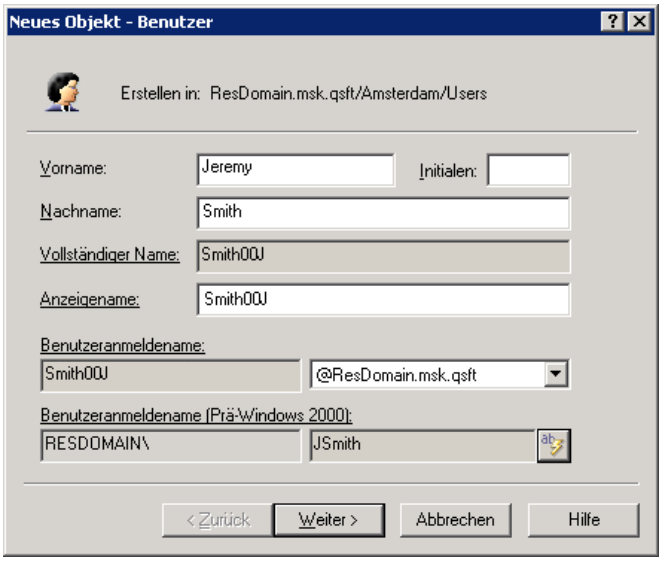
Richtlinien dieser Kategorie dienen zur Generierung von Standardwerten für Eigenschaften bei der Erstellung neuer Verzeichnisobjekte, z.B. Benutzerkonten oder Gruppen. Beim Erstellen oder Ändern von Verzeichnisobjekten wird mit ihnen überprüft, ob Eigenschaftswerte Unternehmensstandards entsprechen.

Sie können für eine beliebige Objekteigenschaft Kriterien angeben, die die Eigenschaftswerte erfüllen müssen, sowie Regeln dafür definieren, welcher Wert der Eigenschaft standardmäßig zugewiesen werden muss. Sie können beispielsweise eine Richtlinie konfigurieren, um eine bestimmte Formatierung von Telefonnummern in Ihrem Verzeichnis durchzusetzen.

Funktionsweise dieser Richtlinie

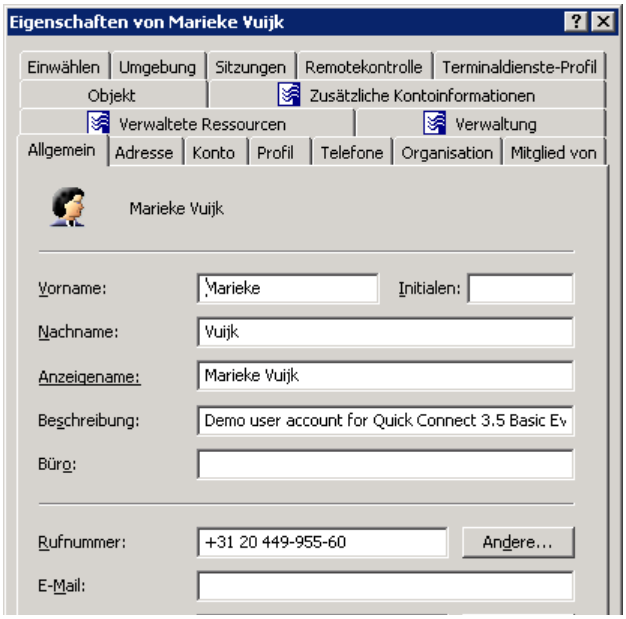
Beim Erstellen oder Ändern eines Objekts überprüft ActiveRoles Server, ob die Eigenschaftswerte die in der Richtlinie definierten Kriterien erfüllen. Wenn sie sie nicht erfüllen, verhindert ActiveRoles Server die Erstellung oder Änderung des Objekts.

In Objekterstellungsassistenten und Eigenschaftsdialogfeldern werden die Eigenschaften, die von der Richtlinie kontrolliert werden, als Hyperlinks angezeigt. Wenn Sie über eine Richtlinie verfügen, die zum Auffüllen einer Eigenschaft mit einem bestimmten Wert (Generieren des Standardwerts) konfiguriert ist, ist das Bearbeitungsfeld für die Eigenschaft nicht zur Bearbeitung verfügbar, wie in der folgenden Abbildung gezeigt.



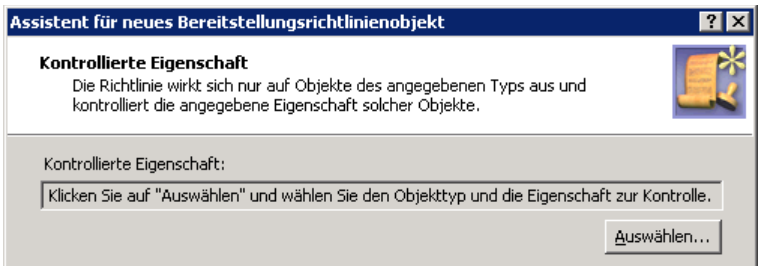
Sie können auf einen Hyperlink klicken, um die Richtliniendetails anzuzeigen.

Wenn eine Richtlinie so konfiguriert ist, dass sie eine Gruppe akzeptabler Werte für eine bestimmt Eigenschaft definiert, stellt die ActiveRoles Server-Konsole ein Dropdown-Listenfeld bereit, in dem Sie beim Ändern dieser Eigenschaft einen Wert auswählen können. Der Benutzer der ActiveRoles Server-Konsole kann somit einen akzeptablen Wert in der Liste auswählen, statt einen Wert in das Bearbeitungsfeld eingeben zu müssen. Diese Funktion wird in der folgenden Abbildung veranschaulicht: Das Feld **Büro** stellt eine Liste der akzeptablen, von der Richtlinie vorgeschriebenen Werte bereit.

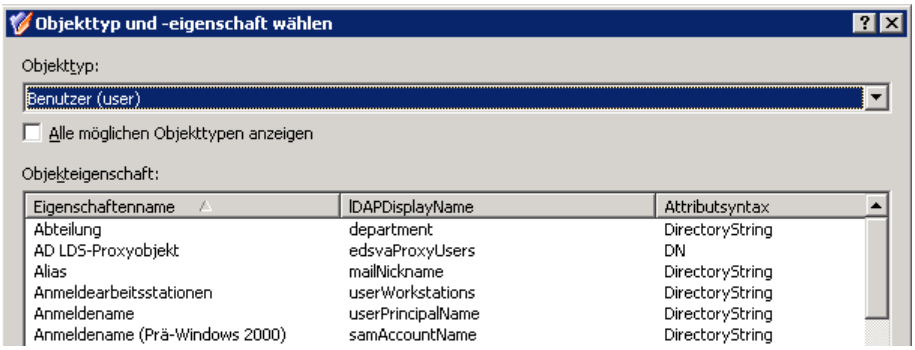


Konfigurieren der Richtlinie „Erzeugung und Validierung von Eigenschaften"

Um die Richtlinie „Erzeugung und Validierung von Eigenschaften" zu konfigurieren, wählen Sie **Erzeugung und Validierung von Eigenschaften** auf der Seite **Zu konfigurierende Richtlinie** im Assistenten für neues Bereitstellungsrichtlinienobjekt oder im Assistenten „Bereitstellungsrichtlinie hinzufügen" aus. Klicken Sie dann auf **Weiter**, damit die Seite **Kontrollierte Eigenschaft** angezeigt wird.

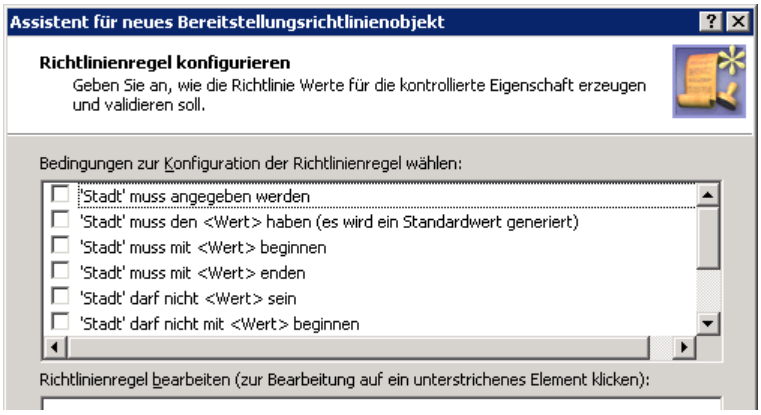

Assistent für neues Bereitstellungsrichtlinienobjekt
Kontrollierte Eigenschaft
Die Richtlinie wirkt sich nur auf Objekte des angegebenen Typs aus und kontrolliert die angegebene Eigenschaft solcher Objekte.
Kontrollierte Eigenschaft:
Klicken Sie auf "Auswählen" und wählen Sie den Objekttyp und die Eigenschaft zur Kontrolle.
Auswählen...

Klicken Sie auf **Auswählen**, um den Objekttyp und die Objekteigenschaft auszuwählen, die die Richtlinie steuern soll. Hierdurch wird das Dialogfeld **Objekttyp und -eigenschaft wählen** angezeigt:



Wählen Sie in der Liste **Objekttyp** den Objekttyp aus: So geben Sie den Typ der Objekte an, die durch die Richtlinie gesteuert werden sollen. Wählen Sie in der Liste **Objekteigenschaft** die Objekteigenschaft aus: So geben Sie die Eigenschaft an, die durch die Richtlinie gesteuert werden soll. Klicken Sie auf **OK**.

Klicken Sie auf der Seite **Kontrollierte Eigenschaft** auf **Weiter**, um die Seite **Richtlinienregel konfigurieren** anzuzeigen.


Assistent für neues Bereitstellungsrichtlinienobjekt
Richtlinienregel konfigurieren
Geben Sie an, wie die Richtlinie Werte für die kontrollierte Eigenschaft erzeugen und validieren soll.
Bedingungen zur Konfiguration der Richtlinienregel wählen:
'Stadt' muss angegeben werden
'Stadt' muss den <Wert> haben (es wird ein Standardwert generiert)
'Stadt' muss mit <Wert> beginnen
'Stadt' muss mit <Wert> enden
'Stadt' darf nicht <Wert> sein
'Stadt' darf nicht mit <Wert> beginnen
Richtlinienregel bearbeiten (zur Bearbeitung auf ein unterstrichenes Element klicken):

Auf dieser Seite können Sie Kriterien bestimmen, mit denen Werte der gesteuerten Eigenschaft generiert und überprüft werden.

Aktivieren Sie zum Konfigurieren einer Richtlinienregel zunächst die entsprechenden Kontrollkästchen im oberen Feld auf der Seite **Richtlinienregel konfigurieren**. Jede Kontrollkästchenbeschriftung besteht aus dem Namen der gesteuerten Eigenschaft, gefolgt von einer Bedingung. Wenn Sie beispielsweise das Kontrollkästchen neben **muss angegeben werden** aktivieren, setzt die Richtlinie durch, dass der Eigenschaft ein Wert zugewiesen wird.

Wenn die Richtlinie einen Standardwert für die gesteuerte Eigenschaft generieren soll, aktivieren Sie das Kontrollkästchen neben **muss den <Wert> haben (es wird ein Standardwert generiert)**.

Wenn die Richtlinie nicht zwischen Groß- und Kleinschreibung unterscheiden soll, aktivieren Sie das Kontrollkästchen neben **ohne Unterscheidung nach Groß-/Kleinschreibung**.

Nach dem Aktivieren von Kontrollkästchen im oberen Feld werden Sie im unteren Feld zum Konfigurieren von Werten aufgefordert, wie in der folgenden Abbildung gezeigt.

Assistent für neues Bereitstellungsrichtlinienobjekt
Richtlinienregel konfigurieren
Geben Sie an, wie die Richtlinie Werte für die kontrollierte Eigenschaft erzeugen und validieren soll.
Bedingungen zur Konfiguration der Richtlinienregel wählen:
'Stadt' muss angegeben werden
'Stadt' muss den <Wert> haben (es wird ein Standardwert generiert)
'Stadt' muss mit <Wert> beginnen
'Stadt' muss mit <Wert> enden
'Stadt' darf nicht <Wert> sein
'Stadt' darf nicht mit <Wert> beginnen
Richtlinienregel bearbeiten (zur Bearbeitung auf ein unterstrichenes Element klicken):
'Stadt' muss angegeben werden und
muss sein:
NewYork (Standardwert) oder
Amsterdam oder
<Zum Hinzufügen des Werts klicken>
Nach der Erstellung eines Objekts generiert diese Richtlinie den folgenden Standardwert:
< Zurück
Weiter >
Abbrechen
Hilfe

Klicken Sie im unteren Feld auf Verknüpfungen mit der Beschriftung **<Zum Hinzufügen des Werts klicken>**, um weitere Werte zu konfigurieren. Wenn Sie im oberen Feld mehrere Kontrollkästchen aktivieren, müssen Sie für jede Bedingung einen Wert konfigurieren.

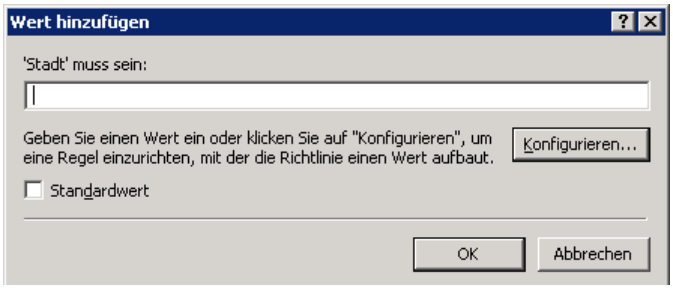
Im Feld **Richtlinienregel bearbeiten** können Sie folgende Aktionen ausführen:

- Ändern eines Wertes. Klicken Sie mit der rechten Maustaste auf den Wert und klicken Sie dann auf **Bearbeiten**. Nun wird ein Dialogfeld ähnlich dem Dialogfeld **Wert hinzufügen** angezeigt, das weiter unten in diesem Abschnitt diskutiert wird.
- Entfernen eines Wertes. Klicken Sie mit der rechten Maustaste auf den Wert, und klicken Sie dann auf **Entfernen**.

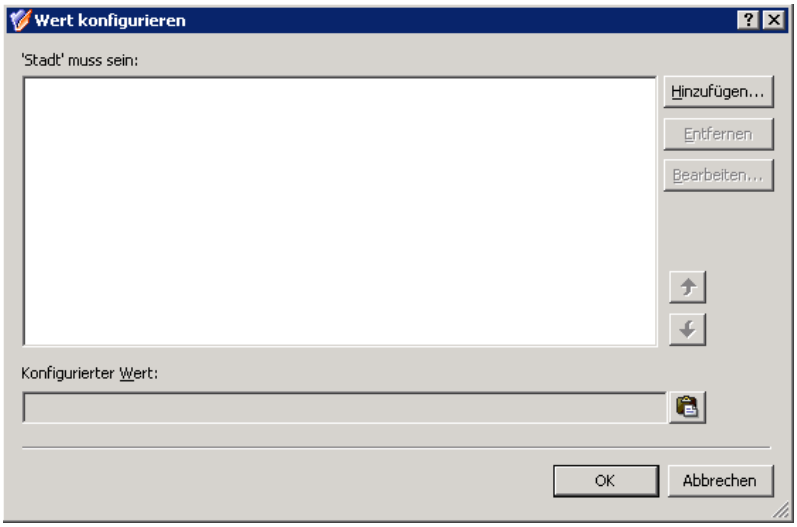
- Neu anordnen der Werteliste (vorausgesetzt, dass mehrere Werte für eine bestimmte Bedingung angegeben sind). Klicken Sie mit der rechten Maustaste auf einen Wert und verwenden Sie den Befehl **Nach oben** bzw. **Nach unten**, um die Position des Werts in der Liste zu ändern, oder klicken Sie auf **Elemente aufsteigend sortieren** bzw. **Elemente absteigend sortieren**, um die Liste entsprechend zu sortieren.
- Importieren von Werten aus einer Textdatei. Bereiten Sie eine Textdatei vor, die einen Wert je Zeile enthält, klicken Sie mit der rechten Maustaste auf einen beliebigen Wert im Feld **Richtlinienregel bearbeiten**, klicken Sie dann auf **Elemente importieren** und öffnen Sie dann die Datei, die Sie vorbereitet haben.
- Exportieren der Werte in eine Textdatei. Klicken Sie mit der rechten Maustaste auf einen beliebigen Wert, klicken Sie auf **Elemente exportieren** und geben Sie eine Textdatei an, in die die Werte geschrieben werden sollen.
- Angeben, ob die Regel den Standardwert generieren soll. Klicken Sie auf die Verknüpfung **Ja** oder **Nein**, um diese Option umzuschalten.

Um Kriterien in der Richtlinienregel zu kombinieren, verwenden Sie die Operatoren UND und ODER. Die Richtlinie wird eingehalten, wenn der Eigenschaftswert alle angegebenen Kriterien (UND) bzw. ein beliebiges von ihnen (ODER) erfüllt. Zum Ändern des Operators klicken Sie auf die Schaltfläche **und** oder **oder**.

Durch Anklicken der Verknüpfung mit dem Namen **<Klicken, um einen Wert hinzuzufügen>** wird ein Dialogfeld angezeigt, dass dem in der folgenden Abbildung gezeigten Dialogfeld entspricht.


Wert hinzufügen
'Stadt' muss sein:
Geben Sie einen Wert ein oder klicken Sie auf "Konfigurieren", um eine Regel einzurichten, mit der die Richtlinie einen Wert aufbaut.
Konfigurieren...
Standardwert
OK
Abbrechen

Im Dialogfeld **Wert hinzufügen** können Sie einen Wert für die ausgewählte Bedingung angeben. Sie können in das Bearbeitungsfeld einen Wert eingeben oder über die Benutzeroberfläche zum Zeigen und Klicken einen Wert konfigurieren. Durch Anklicken der Schaltfläche **Konfigurieren** wird das Dialogfeld **Wert konfigurieren** angezeigt, das in der folgenden Abbildung dargestellt ist.



Jeder Wert entsteht durch Verkettung von mindestens einem Eintrag. Im Dialogfeld **Wert konfigurieren** können Sie folgende Aktionen ausführen:

- Hinzufügen beliebig vieler Einträge zu dem Wert. Klicken Sie auf **Hinzufügen**, um das Fenster **Eintrag hinzufügen** anzuzeigen, das weiter unten in diesem Abschnitt diskutiert wird.
- Entfernen von Einträgen aus dem Wert. Wählen Sie in der Liste Einträge aus, und klicken Sie auf **Entfernen**.
- Ändern von Einträgen im Wert. Wählen Sie einen Eintrag aus, und klicken Sie auf **Bearbeiten**. Nun wird ein Fenster angezeigt, das dem Fenster **Eintrag hinzufügen** ähnelt und in dem Sie die Eintragseigenschaften anzeigen und ändern können.
- Verschieben des ausgewählten Eintrags nach oben oder unten in der Liste, um die Einträge in dem Wert anders anzuordnen. Klicken Sie im oberen Feld auf einen Eintrag, und klicken Sie dann auf die Schaltflächen mit den Pfeilen neben dem Feld, um den Eintrag zu verschieben.
- Einfügen des Textes aus der Zwischenablage am Ende des Wertes. Wenn der Text eine gültige Syntax aufweist, mit der ein Eintrag eines anderen Typs als **Text** implementiert wird (siehe Tabelle unten), wird die Syntax entsprechend behandelt. Kopieren Sie einen Text in die Zwischenablage, und klicken Sie dann auf die Schaltfläche neben dem Feld **Konfigurierter Wert**, um den Text hinter das Ende der Zeichenfolge in diesem Feld einzufügen.

Im Fenster **Eintrag hinzufügen** können Sie den Typ des hinzuzufügenden Eintrags auswählen und den Eintrag dann konfigurieren. In der folgenden Tabelle werden die verfügbaren Eintragstypen zusammengefasst.

EINTRAGSTYP	BESCHREIBUNG
Text	Fügt dem Wert eine Textzeichenfolge hinzu.
<*Objekteigenschaft*>	Fügt eine ausgewählte Eigenschaft des von der Richtlinie verwalteten Objekts (oder einen Teil einer Eigenschaft) hinzu. Wenn ein Eintrag dieses Typs angezeigt wird, ersetzt die Konsole den Platzhalter <*Object*> durch die tatsächliche Kategorie der Objekte, die der Steuerung der Richtlinie unterliegen. Wenn die Richtlinie beispielsweise für die Steuerung einer bestimmten Eigenschaft von Benutzerobjekten konfiguriert ist, können Sie mit Hilfe von Einträgen dieses Typs diese Eigenschaft eines Benutzerobjekts mit Daten aus anderen Eigenschaften des gleichen Benutzerobjekts auffüllen.
Eigenschaft der übergeordneten Organisationseinheit	Fügt eine ausgewählte Eigenschaft (oder einen Teil einer Eigenschaft) einer Organisationseinheit in der Containerhierarchie über dem von dieser Richtlinie verwalteten Objekt hinzu. Wenn die Richtlinie beispielsweise für die Steuerung einer bestimmten Eigenschaft von Benutzerobjekten konfiguriert ist, können Sie mit Hilfe von Einträgen dieses Typs diese Eigenschaft eines Benutzerobjekts mit Daten aus Eigenschaften der Organisationseinheit auffüllen, die dieses Benutzerobjekt enthält (also der unmittelbar übergeordneten Organisationseinheit).
Eigenschaft der übergeordneten Domäne	Fügt eine ausgewählte Eigenschaft (oder einen Teil einer Eigenschaft) der Domäne des von dieser Richtlinie verwalteten Objekts hinzu. Wenn die Richtlinie beispielsweise für die Steuerung einer bestimmten Eigenschaft von Benutzerobjekten konfiguriert ist, können Sie mit Hilfe von Einträgen dieses Typs diese Eigenschaft eines Benutzerobjekts mit Daten auffüllen, die in Eigenschaften der Domäne gespeichert sind, in der sich dieses Benutzerobjekt befindet.
Maske	Fügt eine Syntax hinzu, die bestimmt, welche Zeichen in der von dieser Richtlinie gesteuerten Eigenschaft zulässig sind. Mit Einträgen dieses Typs können Sie ein Datenformat durchsetzen, beispielsweise für Zahlen, Postleitzahlen oder Telefonnummern.

Die Schritte zum Konfigurieren eines Eintrags hängen vom Eintragstyp ab. In den folgenden Abschnitten werden die Vorgehensweisen für jeden der Eintragstypen näher beschrieben, die im Fenster **Eintrag hinzufügen** vorkommen.

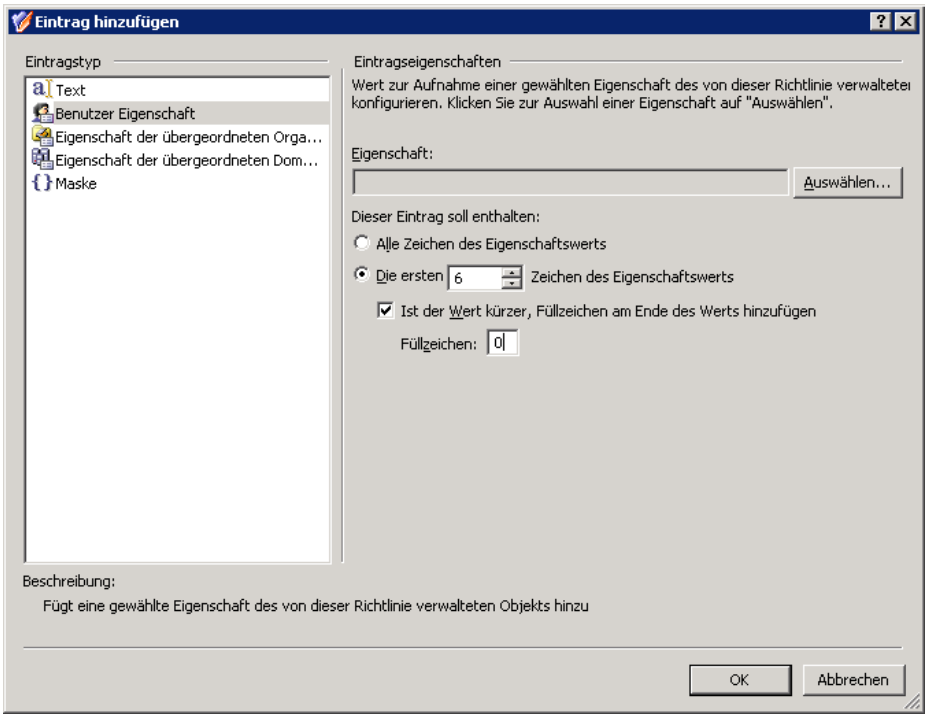
Eintragstyp: Text

Wenn Sie im Fenster **Eintrag hinzufügen** unter **Eintragstyp** den Typ **Text** auswählen, wird im Bereich **Eintragseigenschaften** das Feld **Textwert** angezeigt.

Geben Sie in das Feld **Textwert** den Text ein, den Sie in den Wert einschließen möchten, und klicken Sie dann auf **OK**.

Eintragstyp: <Objekteigenschaft>

Wenn Sie im Fenster **Eintrag hinzufügen** unter **Eintragstyp** den Typ **Eigenschaft des <Objekts>** auswählen, ähnelt der Bereich **Eintragseigenschaften** der folgenden Abbildung.



Mit diesem Eintragstyp können Sie einen Wert konfigurieren, der auf einer Eigenschaft des Objekts selbst basiert. Um eine Eigenschaft auszuwählen, klicken Sie auf **Auswählen**.

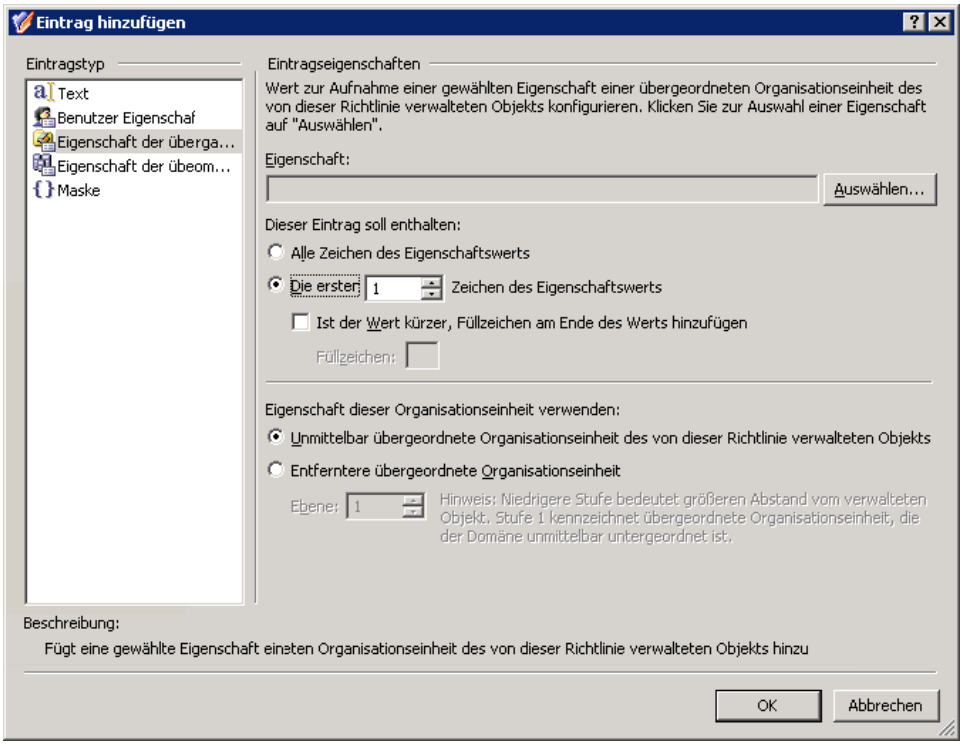
Wenn der Eintrag den gesamten Wert der Eigenschaft enthalten soll, klicken Sie auf **Alle Zeichen des Eigenschaftswerts**. Klicken Sie andernfalls auf **Die ersten**, und geben Sie an, wie viele Zeichen in den Eintrag eingeschlossen werden sollen.

Im letzteren Fall können Sie das Kontrollkästchen **Ist der Wert kürzer, Füllzeichen am Ende des Werts hinzufügen** aktivieren und ein Zeichen in das Feld **Füllzeichen** eingeben. Dieses Zeichen ersetzt die fehlenden Zeichen im Wert der Objekteigenschaft, wenn dieser Wert kürzer ist als im Feld neben der Option **Die ersten** angegeben.

Klicken Sie nach dem Konfigurieren eines Eintrags auf **OK**, um das Fenster **Eintrag hinzufügen** zu schließen. Der Eintrag wird dem Dialogfeld **Wert konfigurieren** hinzugefügt.

Eintragstyp: Eigenschaft der übergeordneten Organisationseinheit

Wenn Sie im Fenster **Eintrag hinzufügen** unter **Eintragstyp** den Typ **Eigenschaft der übergeordneten Organisationseinheit** auswählen, ähnelt der Bereich **Eintragseigenschaften** der folgenden Abbildung.


Eintrag hinzufügen
Eintragstyp
Text
Benutzer Eigenschaf
Eigenschaft der überga...
Eigenschaft der übeom...
Maske
Eintragseigenschaften
Wert zur Aufnahme einer gewählten Eigenschaft einer übergeordneten Organisationseinheit des von dieser Richtlinie verwalteten Objekts konfigurieren. Klicken Sie zur Auswahl einer Eigenschaft auf "Auswählen".
Eigenschaft:
Auswählen...
Dieser Eintrag soll enthalten:
Alle Zeichen des Eigenschaftswerts
Die ersten: 1 Zeichen des Eigenschaftswerts
Ist der Wert kürzer, Füllzeichen am Ende des Werts hinzufügen
Füllzeichen:
Eigenschaft dieser Organisationseinheit verwenden:
Unmittelbar übergeordnete Organisationseinheit des von dieser Richtlinie verwalteten Objekts
Entferntere übergeordnete Organisationseinheit
Ebene: 1
Hinweis: Niedrigere Stufe bedeutet größeren Abstand vom verwalteten Objekt. Stufe 1 kennzeichnet übergeordnete Organisationseinheit, die der Domäne unmittelbar untergeordnet ist.
Beschreibung:
Fügt eine gewählte Eigenschaft einsten Organisationseinheit des von dieser Richtlinie verwalteten Objekts hinzu
OK
Abbrechen

Mit diesem Eintragstyp können Sie einen Wert konfigurieren, der auf einer Eigenschaft einer übergeordneten Organisationseinheit des von dieser Richtlinie verwalteten Objekts basiert. Um eine Eigenschaft einer Organisationseinheit auszuwählen, klicken Sie auf **Auswählen**.

Wenn der Eintrag den gesamten Wert der Eigenschaft enthalten soll, klicken Sie auf **Alle Zeichen des Eigenschaftswerts**. Klicken Sie andernfalls auf **Die ersten**, und geben Sie an, wie viele Zeichen in den Eintrag eingeschlossen werden sollen.

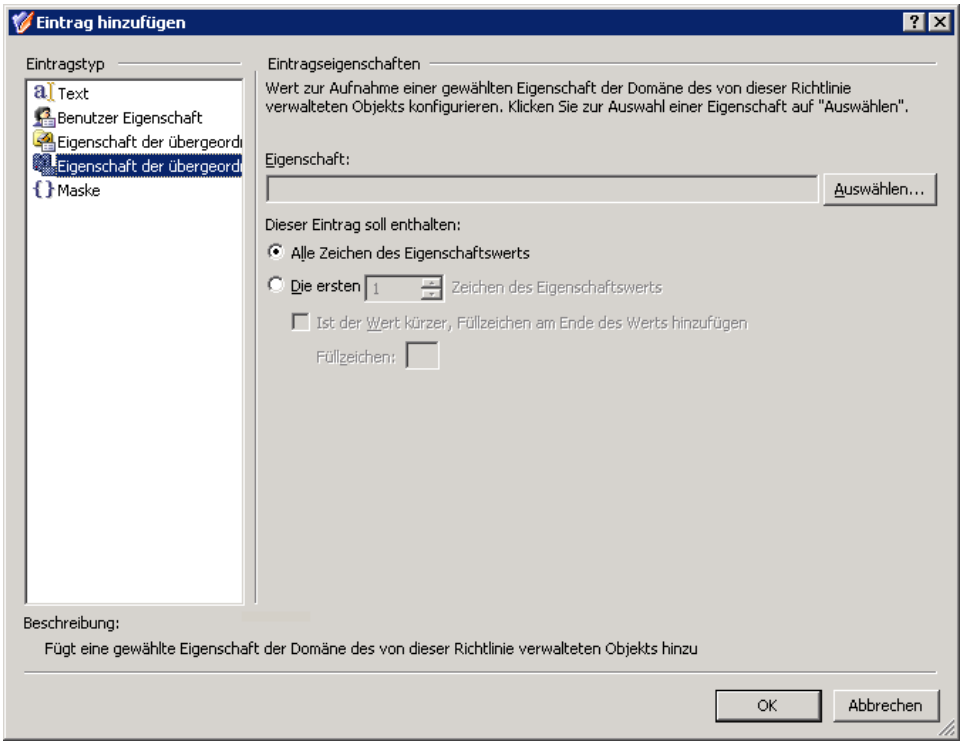
Im letzteren Fall können Sie das Kontrollkästchen **Ist der Wert kürzer, Füllzeichen am Ende des Werts hinzufügen** aktivieren und ein Zeichen in das Feld **Füllzeichen** eingeben. Dieses Zeichen ersetzt die fehlenden Zeichen im Wert der Organisationseinheitseigenschaft, wenn dieser Wert kürzer ist als im Feld neben der Option **Die ersten** angegeben.

Sie können auch die Ebene der Organisationseinheit angeben, die von der Richtlinie verwendet werden soll. Um die Eigenschaft der Organisationseinheit zu verwenden, in der sich das Objekt befindet, klicken Sie auf **Unmittelbar übergeordnete Organisationseinheit des von dieser Richtlinie verwalteten Objekts**. Um die Eigenschaft einer übergeordneten Organisationseinheit einer anderen Ebene zu verwenden, klicken Sie auf **Entferntere übergeordnete Organisationseinheit**, und geben Sie dann im Feld **Ebene** die Ebene der Organisationseinheit an. Eine tiefere Ebene bedeutet eine größere Entfernung vom verwalteten Objekt in der Containerhierarchie über diesem Objekt. Die Ebene 1 bedeutet eine unmittelbar untergeordnete Organisationseinheit der Domäne.

Klicken Sie nach dem Konfigurieren eines Eintrags auf **OK**, um das Fenster **Eintrag hinzufügen** zu schließen. Der Eintrag wird dem Dialogfeld **Wert konfigurieren** hinzugefügt.

Eintragstyp: Eigenschaft der übergeordneten Domäne

Wenn Sie im Fenster **Eintrag hinzufügen** unter **Eintragstyp** den Typ **Eigenschaft der übergeordneten Domäne** auswählen, ähnelt der Bereich **Eintragseigenschaften** der folgenden Abbildung.


Eintrag hinzufügen
Eintragstyp
Text
Benutzer Eigenschaft
Eigenschaft der übergeordn
Eigenschaft der übergeordn
Maske
Eintragseigenschaften
Wert zur Aufnahme einer gewählten Eigenschaft der Domäne des von dieser Richtlinie verwalteten Objekts konfigurieren. Klicken Sie zur Auswahl einer Eigenschaft auf "Auswählen".
Eigenschaft:
Auswählen...
Dieser Eintrag soll enthalten:
Alle Zeichen des Eigenschaftswerts
Die ersten 1 Zeichen des Eigenschaftswerts
Ist der Wert kürzer, Füllzeichen am Ende des Werts hinzufügen
Füllzeichen:
Beschreibung:
Fügt eine gewählte Eigenschaft der Domäne des von dieser Richtlinie verwalteten Objekts hinzu
OK
Abbrechen

Mit diesem Eintragstyp können Sie einen Wert konfigurieren, der auf einer Eigenschaft der Domäne des von dieser Richtlinie verwalteten Objekts basiert. Um eine Domäneneigenschaft auszuwählen, klicken Sie auf **Auswählen**.

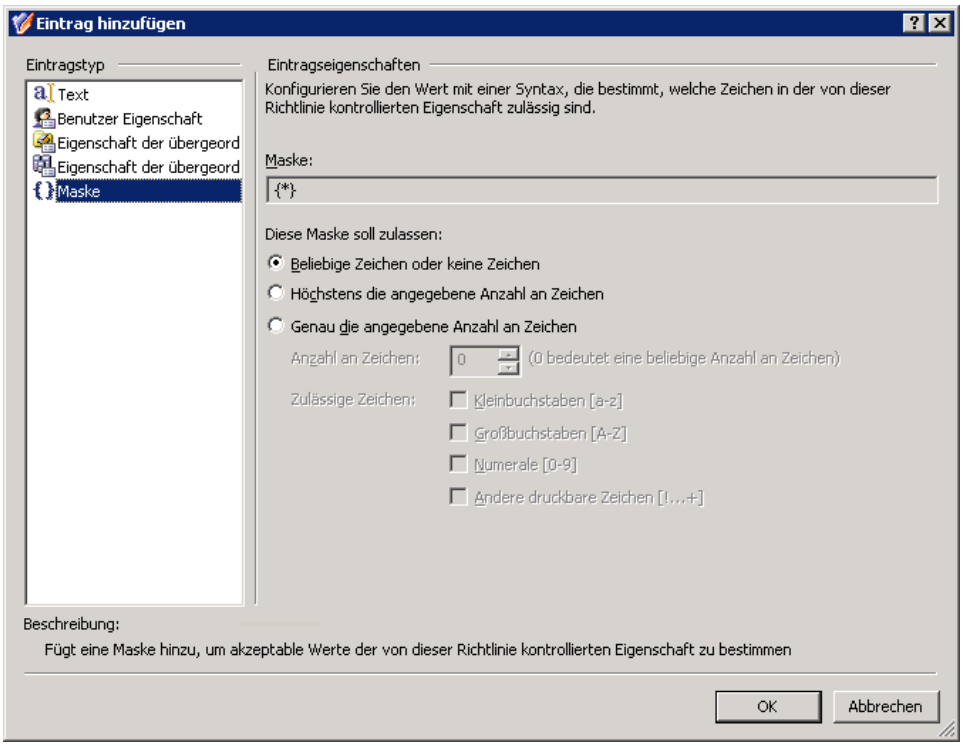
Wenn der Eintrag den gesamten Wert der Eigenschaft enthalten soll, klicken Sie auf **Alle Zeichen des Eigenschaftswerts**. Klicken Sie andernfalls auf **Die ersten**, und geben Sie an, wie viele Zeichen in den Eintrag eingeschlossen werden sollen.

Im letzteren Fall können Sie das Kontrollkästchen **Ist der Wert kürzer, Füllzeichen am Ende des Werts hinzufügen** aktivieren und ein Zeichen in das Feld **Füllzeichen** eingeben. Dieses Zeichen ersetzt die fehlenden Zeichen im Wert der Domäneneigenschaft, wenn dieser Wert kürzer ist als im Feld neben der Option **Die ersten** angegeben.

Klicken Sie nach dem Konfigurieren eines Eintrags auf **OK**, um das Fenster **Eintrag hinzufügen** zu schließen. Der Eintrag wird dem Dialogfeld **Wert konfigurieren** hinzugefügt.

Eintragstyp: Maske

Wenn Sie im Fenster **Eintrag hinzufügen** unter **Eintragstyp** den Typ **Maske** auswählen, ähnelt der Bereich **Eintragseigenschaften** der folgenden Abbildung.



Mit diesem Eintragstyp können Sie definieren, welche Zeichen (Buchstaben, Ziffern) in dem Eintrag zulässig sind, den Sie dem Wert der gesteuerten Eigenschaft hinzufügen.

Wenn Sie für den Eintrag beliebige Folgen von Zeichen zulassen möchten, klicken Sie auf **Beliebige Zeichen oder keine Zeichen**.

Wenn Sie eine Maximalzahl zulässiger Zeichen im Eintrag angeben möchten, klicken Sie auf **Höchstens die angegebene Anzahl an Zeichen**. Geben Sie im Feld **Anzahl an Zeichen** die Anzahl zulässiger Zeichen an. Der Eintrag kann beliebig viele Zeichen bis hin zur angegebenen Anzahl enthalten. Aktivieren Sie unter **Zulässige Zeichen** Kontrollkästchen, um die zulässigen Zeichen anzugeben.

Wenn Sie eine genaue Anzahl im Eintrag erforderlicher Zeichen angeben möchten, klicken Sie auf **Genau die angegebene Anzahl an Zeichen**. Geben Sie im Feld **Anzahl an Zeichen** die Anzahl zulässiger Zeichen an. Der Eintrag muss genau die angegebene Anzahl von Zeichen enthalten. Aktivieren Sie unter **Zulässige Zeichen** Kontrollkästchen, um die zulässigen Zeichen anzugeben.

Klicken Sie nach dem Konfigurieren eines Eintrags auf **OK**, um das Fenster **Eintrag hinzufügen** zu schließen. Der Eintrag wird dem Dialogfeld **Wert konfigurieren** hinzugefügt.

Klicken Sie nach dem Konfigurieren eines Wertes auf **OK**, um das Dialogfeld **Wert konfigurieren** zu schließen, und klicken Sie dann im Dialogfeld **Wert hinzufügen** auf **OK**. Damit wird der Wert zur Eigenschaftsrichtlinie hinzugefügt.

Klicken Sie nach dem Konfigurieren der Richtlinienregeln auf der Seite **Richtlinienregel konfigurieren** auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schrittweise Anleitungen finden Sie unter **Anleitungen/Verwalten von Richtlinienobjekten/ Konfigurieren von Bereitstellungsrichtlinienobjekten/Konfigurieren einer Eigenschaftsgenerierungs- und -überprüfungsrichtlinie** in der ActiveRoles Server-Hilfe.

Szenario 1: Durchsetzen eines Formats für Telefonnummern mit Hilfe einer Maske

In diesem Szenario wird beschrieben, wie Sie eine Richtlinie konfigurieren, die für die Telefonnummern von Benutzern das Format (###) ###-##-## durchsetzt.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen und konfigurieren Sie ein Richtlinienobjekt, das die entsprechende Richtlinie definiert.
2. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Folglich überprüft ActiveRoles Server beim Erstellen oder Ändern eines Benutzerobjekts in dem in Schritt 2 ausgewählten Container, ob die Telefonnummer dem angegebenen Format entspricht. Wenn sie ihm nicht entspricht, verbietet die Richtlinie die Erstellung oder Änderung des Benutzerobjekts.

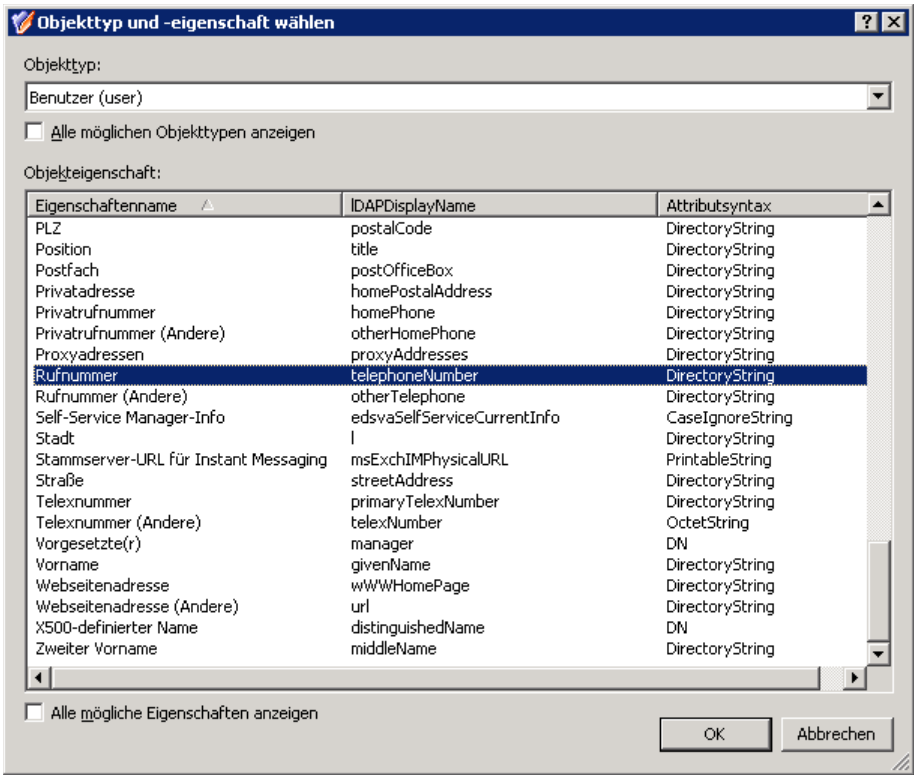
In den folgenden beiden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen und Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt mit dem Assistenten für neues Bereitstellungsrichtlinienobjekt erstellen und konfigurieren. Weitere Informationen über den Assistenten finden Sie unter „Erstellen eines Richtlinienobjekts“ im Abschnitt „Verwaltungsaufgaben für Richtlinienobjekte“ weiter oben in diesem Kapitel.

Klicken Sie zum Konfigurieren der Richtlinie auf der Seite **Zu konfigurierende Richtlinie** des Assistenten auf **Erzeugung und Validierung von Eigenschaften**. Klicken Sie dann auf **Weiter**.

Klicken Sie auf der Seite **Kontrollierte Eigenschaft** auf **Auswählen**. Wählen Sie dann im Dialogfeld **Objekttyp und -eigenschaft wählen** in der Liste **Objekttyp** den Eintrag **Benutzer** aus, und klicken Sie in der Liste **Objekteigenschaft** auf **Rufnummer**, wie in der folgenden Abbildung gezeigt.

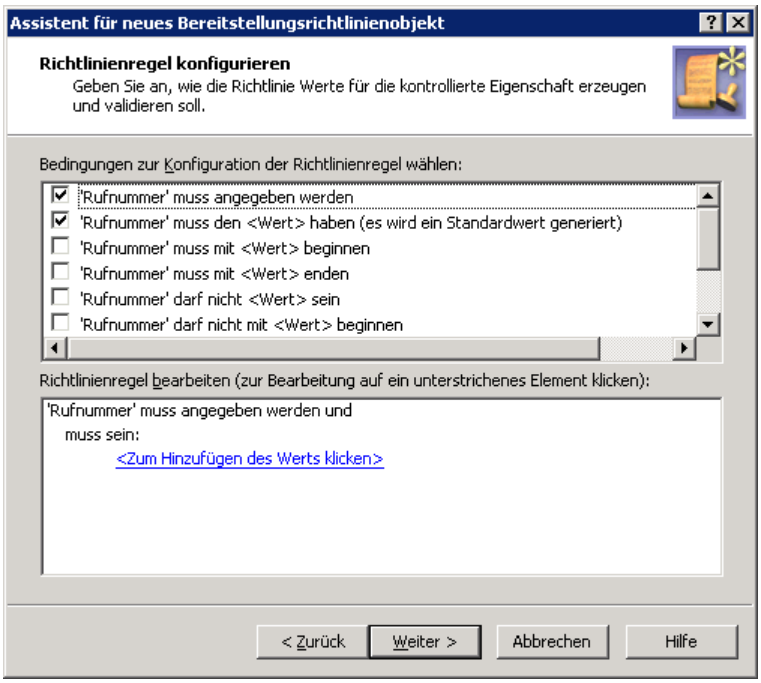


Klicken Sie auf **OK** und dann auf **Weiter**.

Aktivieren Sie auf der Seite **Richtlinienregel konfigurieren** im oberen Feld die folgenden Kontrollkästchen:

- **„Rufnummer" muss angegeben werden** (somit ist die Telefonnummer eine erforderliche Eigenschaft, es muss also in jedem Benutzerkonto eine Telefonnummer angegeben werden).
- **„Rufnummer" muss den <Wert> haben** (mit dieser Option können Sie eine Maske für die Telefonnummer konfigurieren, indem Sie dem Wert für diese Bedingung den entsprechenden Eintrag hinzufügen).

Nun entspricht die Seite **Richtlinienregeln konfigurieren** der folgenden Abbildung.



In der nächsten Phase wird der Wert konfiguriert.

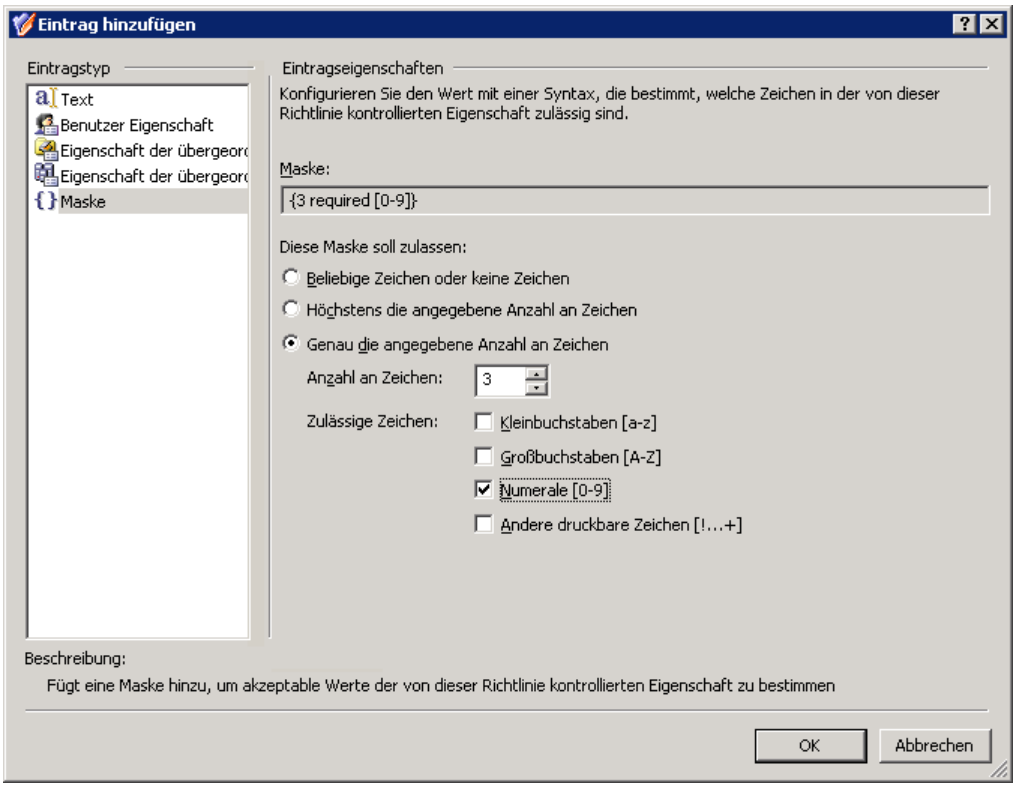
Klicken Sie auf die Verknüpfung mit der Beschriftung **<Zum Hinzufügen des Werts klicken>**. Klicken Sie im Dialogfeld **Wert hinzufügen** auf **Konfigurieren**. Klicken Sie im Dialogfeld **Wert konfigurieren** auf **Hinzufügen**. Klicken Sie im Fenster **Eintrag hinzufügen** unter **Eintragstyp** auf **Maske**.

Jetzt können Sie im Fenster **Eintrag hinzufügen** im Bereich **Eintragseigenschaften** eine Maske konfigurieren.

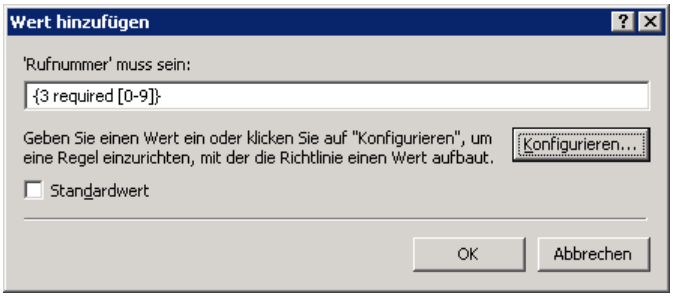
Das Format besteht aus vier Gruppen von Ziffern, die durch bestimmte Zeichen getrennt sind: Leerzeichen, Bindestriche und Klammern. Konfigurieren Sie zuerst eine Maske, die festlegt, dass die ersten drei Zeichen Ziffern sein müssen:

- Wählen Sie **Genau die angegebene Anzahl an Zeichen** aus.
- Geben Sie in das Feld **Anzahl an Zeichen** den Wert **3** ein.
- Aktivieren Sie unter **Zulässige Zeichen** das Kontrollkästchen **Zahlen**.

Das Fenster **Eintrag hinzufügen** sollte nun der folgenden Abbildung entsprechen.



Klicken Sie auf **OK**, um das Fenster **Eintrag hinzufügen** zu schließen. Klicken Sie dann auf **OK**, um das Dialogfeld **Wert konfigurieren** zu schließen. Nunmehr sollte das Dialogfeld **Wert hinzufügen** der folgenden Abbildung entsprechen.

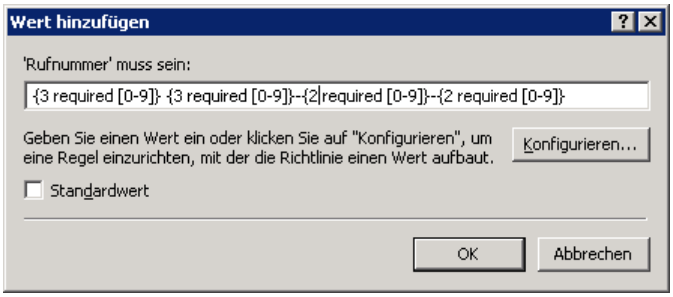

Wert hinzufügen
'Rufnummer' muss sein:
{3 required [0-9]}
Geben Sie einen Wert ein oder klicken Sie auf "Konfigurieren", um eine Regel einzurichten, mit der die Richtlinie einen Wert aufbaut.
Konfigurieren...
Standardwert
OK
Abbrechen

Sie können nun im Dialogfeld **Wert hinzufügen** die Maske bearbeiten.

Anhand der bereits konfigurierten Maske können Sie ahnen, dass Sie für das Telefonnummerformat folgende Maske benötigen:

```
({3 required [0-9]}) {3 required [0-9]}-{2 required [0-9]}-{2 required [0-9]}
```

Geben Sie diese Maske im Dialogfeld **Wert hinzufügen** in das Feld **„Rufnummer" muss sein** ein. Beachten Sie, dass die ersten drei Zeichen in runde Klammern eingeschlossen sind, dann ein Leerzeichen folgt, und dass zwei Bindestriche die Zeichengruppen trennen:


Wert hinzufügen
'Rufnummer' muss sein:
{3 required [0-9]} {3 required [0-9]}--{2 required [0-9]}--{2 required [0-9]}
Geben Sie einen Wert ein oder klicken Sie auf "Konfigurieren", um eine Regel einzurichten, mit der die Richtlinie einen Wert aufbaut.
Konfigurieren...
Standardwert
OK
Abbrechen

Klicken Sie auf **OK**, um das Dialogfeld **Wert hinzufügen** zu schließen. Klicken Sie auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schritt 2: Anwenden des Richtlinienobjekts

Sie können das Richtlinienobjekt mit Hilfe der Seite **Richtlinie erzwingen** im Assistenten für neues Bereitstellungsrichtlinienobjekt anwenden oder Sie können den Assistenten erst abschließen und dann den Befehl **Richtlinie erzwingen** für die Domäne, die Organisationseinheit oder die verwaltete Einheit verwenden, auf die Sie die Richtlinie anwenden möchten.

Weitere Informationen über die Anwendung eines Richtlinienobjekts finden Sie unter „Anwenden von Richtlinienobjekten" und „Verwalten des Richtlinienbereichs" weiter oben in diesem Kapitel.

Szenario 2: Durchsetzen eines Formats für Telefonnummern mit Hilfe regulärer Ausdrücke

In diesem Szenario wird beschrieben, wie Sie eine Richtlinie konfigurieren, die für die Telefonnummern von Benutzern das folgende Format durchsetzt:

- Das erste Zeichen muss „+" lauten
- Das bzw. die folgende(n) Zeichen müssen den Ländercode darstellen
- (Dieser lautet 1 in den USA und in Kanada, und beispielsweise in Australien 61)
- Die Vorwahl für die Stadt/Region muss mit Leerzeichen (und nicht mit Bindestrichen oder Klammern) abgetrennt sein
- Die Telefonnummer muss mit Leerzeichen (und nicht mit Bindestrichen) abgetrennt sein
- Optional kann die Durchwahl mit einem kleinen „x" angegeben werden

Die folgende Tabelle enthält Beispiele, die zeigen, wie die Telefonnummer anhand dieser Formatierungsanforderungen dargestellt werden muss.

RICHTIG	FALSCH	KOMMENTAR
+1 949 754 8515	949-754-8515	Der falsche Eintrag beginnt nicht mit „+" und dem Ländercode. Außerdem enthält er Bindestriche statt Leerzeichen.
+44 1628 606699 x1199	+44 1628 606699 X1199	Der falsche Eintrag enthält den Großbuchstaben X.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Konfigurieren Sie das Richtlinienobjekt, das die entsprechende Richtlinie definiert.
2. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Folglich überprüft ActiveRoles Server beim Erstellen oder Ändern eines Benutzerobjekts in dem in Schritt 2 ausgewählten Container, ob die Telefonnummer dem angegebenen Format entspricht. Wenn sie ihm nicht entspricht, verbietet die Richtlinie die Erstellung oder Änderung des Benutzerobjekts.

Schritt 1: Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt konfigurieren, indem Sie das Richtlinienobjekt ändern, das das vorige Szenario implementiert; siehe „Szenario 1: Durchsetzen eines Formats für Telefonnummern mit Hilfe einer Maske" weiter oben in diesem Abschnitt.

Zeigen Sie das Dialogfeld **Eigenschaften** für dieses Richtlinienobjekt an und öffnen Sie die Registerkarte **Richtlinien**. Wählen Sie dann in der Liste die Richtlinie aus, und klicken Sie auf **Anzeigen/Bearbeiten**, um das Dialogfeld **Eigenschaften der Eigenschaftsgenerierungs- und -validierungsrichtlinie** anzuzeigen.

Die Registerkarte **Richtlinienregel** im Dialogfeld **Eigenschaften der Eigenschaftsgenerierungs- und -validierungsrichtlinie** ähnelt der Seite **Richtlinienregel konfigurieren** des Assistenten, mit dem Sie die Richtlinie konfiguriert haben. Auf dieser Registerkarte können Sie die Richtlinienregeln ändern.

Ändern Sie die Regel zunächst, indem Sie den Maskeneintrag entfernen. Deaktivieren Sie auf der Registerkarte **Richtlinienregel** im oberen Feld das Kontrollkästchen **„Rufnummer" muss <Wert> sein**.

Wählen Sie dann aus, dass die Regel anhand regulärer Ausdrücke konfiguriert werden soll. Aktivieren Sie auf der Registerkarte **Richtlinienregel** im oberen Feld das Kontrollkästchen **„Rufnummer" muss regulärer Ausdruck <Wert> sein**. Um auf dieses Kontrollkästchen zuzugreifen, müssen Sie in der Liste der Kontrollkästchen einen Bildlauf nach unten ausführen.

Geben Sie zum Schluss die regulären Ausdrücke an, die die betreffende Richtlinie definieren. Sie benötigen folgende reguläre Ausdrücke:

```
^\+([0-9]+ )+[0-9]+$
^\+([0-9]+ )+x[0-9]+$
```

Die folgende Tabelle enthält eine kurze Beschreibung der Elemente, die in den beiden Syntaxzeichenfolgen oben verwendet werden. Weitere Informationen über reguläre Ausdrücke finden Sie in „Anhang A: Verwenden von regulären Ausdrücken" weiter unten in diesem Dokument.

ELEMENT	BEDEUTUNG
^	Der Anfang der zu überprüfenden Eingabezeichenfolge.
\+	Die Escapezeichenfolge zur Darstellung des Pluszeichens (+).
([0-9]+)+	Eine Verkettung von mindestens einer Teilzeichenfolge. Dabei besteht jede Teilzeichenfolge aus mindestens einer Ziffer, gefolgt von einem Leerzeichen.
[0-9]+	Mindestens eine Ziffer.
x[0-9]+	Der Kleinbuchstabe „x" gefolgt von mindestens einer Ziffer.
$	Das Ende der zu überprüfenden Eingabezeichenfolge.

Die Richtlinie muss also so konfiguriert werden, dass nur Telefonnummern zugelassen werden, die dem Ausdruck ^\+([0-9]+)+[0-9]+$ (ohne Durchwahl) oder ^\+([0-9]+)+x[0-9]+$ (mit Durchwahl) entsprechen. Konfigurieren Sie die Richtlinie desweiteren wie folgt:

1. Klicken Sie auf der Registerkarte **Richtlinienregel** im unteren Feld auf die Verknüpfung mit der Beschriftung **<Zum Hinzufügen des Werts klicken>**.
2. Geben Sie im Dialogfeld **Wert hinzufügen ^\+([0-9]+)+[0-9]+$** ein und klicken Sie dann auf **OK**.
3. Klicken Sie auf der Registerkarte **Richtlinienregel** im unteren Feld auf die Verknüpfung mit der Beschriftung **<Zum Hinzufügen des Werts klicken>**.
4. Geben Sie im Dialogfeld **Wert hinzufügen ^\+([0-9]+)+x[0-9]+$** ein und klicken Sie dann auf **OK**.
5. Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften der Eigenschaftsgenerierungs- und -validierungsrichtlinie** zu schließen.

Schritt 2: Anwenden des Richtlinienobjekts

Sie können das Richtlinienobjekt anwenden, ohne das zugehörige Dialogfeld **Eigenschaften** zu schließen. Rufen Sie die Registerkarte **Bereich** auf und gehen Sie folgendermaßen vor:

1. Klicken Sie auf der Registerkarte **Bereich** auf die Schaltfläche **Bereich**, um das Fenster **ActiveRoles Serverrichtlinienbereich** für das zu verwaltende Richtlinienobjekt anzuzeigen.
2. Klicken Sie auf **Hinzufügen** und wählen Sie die Domäne, Organisationseinheit oder verwaltete Einheit aus, auf die Sie die Richtlinie anwenden möchten.

   *Sie können auch mit Hilfe der Schaltfläche **Entfernen** Elemente entfernen, auf die die Richtlinie nicht mehr angewendet werden soll.*
3. Klicken Sie auf **OK**, um das Fenster **ActiveRoles Serverrichtlinienbereich** zu schließen.
4. Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften** für das Richtlinienobjekt zu schließen.

Weitere Informationen über die Anwendung eines Richtlinienobjekts finden Sie unter „Anwenden von Richtlinienobjekten“ und „Verwalten des Richtlinienbereichs“ weiter oben in diesem Kapitel.

Erzeugung von Benutzeranmeldenamen

Mit Richtlinien dieser Kategorie kann bei der Erstellung oder Änderung eines Benutzerkontos die Zuweisung des Benutzer-Anmeldenamens (Prä-Windows 2000) automatisiert werden. Dabei stehen flexible Optionen zur Verfügung, um die Eindeutigkeit des von Richtlinien generierten Namens sicherzustellen.

Es ist sehr wichtig, dass ein eindeutiger Name generiert werden kann. Wenn ActiveRoles Server versucht, einen von einer Richtlinie generierten Namen zuzuweisen, wenn bereits ein Benutzerkonto mit demselben Benutzer-Anmeldenamen (Prä-Windows 2000) vorhanden ist, tritt ein Namenskonflikt auf. Active Directory unterstützt nicht mehrere Konten mit demselben Benutzer-Anmeldenamen (Prä-Windows 2000). Eine Richtlinie kann so konfiguriert werden, dass sie eine Serie von Namen generiert, damit keine Namenskonflikte mit vorhandenen Konten auftreten.

Beim Konfigurieren einer Richtlinie dieser Kategorie können Sie mehrere Regeln definieren, die die Richtlinie bei einem Namenskonflikt nacheinander anwendet, um einen eindeutigen Namen zu generieren. Sie können auch eine Regel konfigurieren, mit der ein inkrementeller numerischer Wert eingeschlossen wird, um die Eindeutigkeit des von der Richtlinie konfigurierten Namens sicherzustellen. Außerdem besteht die Option, zuzulassen, dass Operatoren beim Erstellen oder Aktualisieren von Benutzerkonten die von Richtlinien konfigurierten Namen ändern.

Funktionsweise dieser Richtlinie

Beim Erstellen eines Benutzerkontos verwendet ActiveRoles Server diese Richtlinie, um dem Benutzerkonto einen bestimmten Namen von Versionen Prä-Windows 2000 zuzuweisen. Die Richtlinie generiert den Namen anhand der Eigenschaften des zu erstellenden Benutzerkontos. Eine Richtlinie kann mindestens eine Regel einschließen, die die Namenswerte als Verkettung von Einträgen konstruiert, die denen der Richtlinie „Erzeugung und Validierung von Eigenschaften" ähneln.

Ein besonderer Eintrag, die Eindeutigkeitszahl, wird bereitgestellt, um den von der Richtlinie generierten Namen eindeutig zu machen. Ein Eindeutigkeitszahleintrag stellt einen numerischen Wert dar, den die Richtlinie im Fall eines Namenskonflikts erhöht. Beispielsweise kann eine Richtlinie die Option bereitstellen, den neuen Namen von JSmith in J1Smith zu ändern, wenn bereits ein Benutzerkonto vorhanden ist, dessen Benutzer-Anmeldename (Prä-Windows 2000) auf JSmith festgelegt ist. Wenn auch der Name J1Smith bereits verwendet wird, kann der neue Name auf J2Smith geändert werden, und so weiter.

Bei der Richtlinienkonfiguration besteht die Option, die manuelle Bearbeitung von Namen, die durch Richtlinien generiert wurden, zuzulassen oder zu verweigern. Die Berechtigung zum Ändern eines Namens, der durch eine Richtlinie generiert wurde, kann auf den Fall eingeschränkt werden, dass der Name von einem anderen Konto verwendet wird.

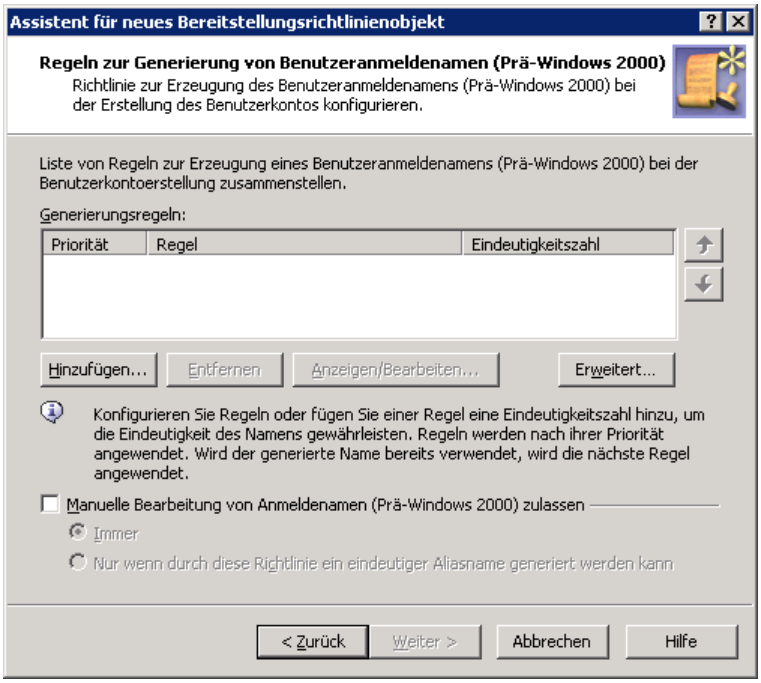
Es folgen einige spezifische Aspekte des Richtlinienverhaltens:

- Mit einer einzelnen Regel, die keine Eindeutigkeitszahl verwendet, versucht ActiveRoles Server einfach, dem Benutzerkonto den generierten Namen zuzuweisen. Der Vorgang schlägt möglicherweise fehl, wenn der generierte Name nicht eindeutig ist, wenn also derselbe Benutzer-Anmeldename (Prä-Windows 2000) bereits einem anderen Benutzerkonto zugewiesen ist. Wenn die Richtlinie die manuelle Bearbeitung von Namen zulässt, die sie generiert hat, kann der Name von dem Operator korrigiert werden, der das Benutzerkonto erstellt.
- Wenn mehrere Regeln oder eine Regel mit Eindeutigkeitszahlen vorliegen, wird in ActiveRoles Server auf der Clientseite auf den Formularen für die Benutzererstellung und -änderung neben dem Feld **Benutzeranmeldename (Prä-Windows 2000)** eine Schaltfläche hinzugefügt.
- Um einen Namen zu generieren, muss der Clientbenutzer (Operator) auf diese Schaltfläche klicken, die auch die Situation abdeckt, in der der generierte Name bereits verwendet wird. Wenn Sie auf die Schaltfläche **Generieren** klicken, wird die nächste Regel angewendet, oder die Eindeutigkeitszahl wird um 1 erhöht, sodass ein eindeutiger Name vergeben werden kann.
- Die Richtlinie definiert eine Liste von Zeichen, die in Benutzer-Anmeldenamen (Prä-Windows 2000) nicht zulässig sind. Die folgenden Zeichen sind nicht zulässig: " / \ [ ] : ; | = , + * ? < >

- Die Richtlinie führt dazu, dass ActiveRoles Server die Verarbeitung von Vorgangsanforderungen ablehnt, die dem Benutzer-Anmeldenamen von Versionen Prä-Windows 2000 einen leeren Wert zuweisen würden.
- Bei der Überprüfung von Benutzerkonten auf die Richtlinieneinhaltung (siehe weiter unten in diesem Dokument) erkennt und berichtet ActiveRoles Server die Benutzer-Anmeldenamen (Prä-Windows 2000), die nicht so eingerichtet sind, wie die Richtlinie „Erzeugung von Benutzeranmeldenamen" vorschreibt.

Konfigurieren der Richtlinie „Erzeugung von Benutzeranmeldenamen"

Um die Richtlinie „Erzeugung von Benutzeranmeldenamen" zu konfigurieren, wählen Sie **Erzeugung von Benutzeranmeldenamen** auf der Seite **Zu konfigurierende Richtlinie** im Assistenten für neues Bereitstellungsrichtlinienobjekt oder im Assistenten „Bereitstellungsrichtlinie hinzufügen" aus. Klicken Sie dann auf **Weiter**, um die Seite **Regeln zur Generierung von Benutzeranmeldenamen (Prä-Windows 2000)** anzuzeigen:


Assistent für neues Bereitstellungsrichtlinienobjekt
Regeln zur Generierung von Benutzeranmeldenamen (Prä-Windows 2000)
Richtlinie zur Erzeugung des Benutzeranmeldenamens (Prä-Windows 2000) bei der Erstellung des Benutzerkontos konfigurieren.
Liste von Regeln zur Erzeugung eines Benutzeranmeldenamens (Prä-Windows 2000) bei der Benutzerkontoerstellung zusammenstellen.
Generierungsregeln:
Priorität
Regel
Eindeutigkeitszahl
Hinzufügen...
Entfernen
Anzeigen/Bearbeiten...
Erweitert...
Konfigurieren Sie Regeln oder fügen Sie einer Regel eine Eindeutigkeitszahl hinzu, um die Eindeutigkeit des Namens gewährleisten. Regeln werden nach ihrer Priorität angewendet. Wird der generierte Name bereits verwendet, wird die nächste Regel angewendet.
Manuelle Bearbeitung von Anmeldenamen (Prä-Windows 2000) zulassen
Immer
Nur wenn durch diese Richtlinie ein eindeutiger Aliasname generiert werden kann
< Zurück
Weiter >
Abbrechen
Hilfe

Auf der Seite **Regeln zur Generierung von Benutzeranmeldenamen (Prä-Windows 2000)** können Sie eine Liste von Generierungsregeln einrichten. Jeder Eintrag in der Liste schließt die folgenden Informationen ein:

- **Priorität** Die Richtlinie wendet Generierungsregeln in der Reihenfolge ihrer Priorität an, die durch ihre Position in der Liste bestimmt wird: Sie werden in der Reihenfolge angewendet, in der sie gelesen werden.
- **Regel** Die Syntax, die die Regel definiert.
- **Eindeutigkeitszahl** Zeigt **Ja** oder **Nein** an, um anzugeben, ob die Regel einen Eindeutigkeitszahleintrag enthält.

Sie können die Liste der Regeln mit folgenden Schaltflächen verwalten:

- **Hinzufügen** Öffnet das Dialogfeld **Wert konfigurieren**, das weiter oben in diesem Kapitel beschrieben wurde (siehe „Konfigurieren einer Richtlinie für die Generierung und Validierung von Eigenschaften"). In diesem Dialogfeld können Sie einen Wert für die Bedingung **„Anmeldename (Prä-Windows 2000)" muss sein** konfigurieren, ähnlich wie beim Konfigurieren der Richtlinie „Erzeugung und Validierung von Eigenschaften". Ausführlichere Informationen finden Sie unter „Konfigurieren einer Generierungsrichtlinie für Anmeldenamen" weiter unten in diesem Abschnitt.
- **Entfernen** Löscht die ausgewählten Regeln aus der Liste.
- **Anzeigen/Bearbeiten** Öffnet das Dialogfeld **Wert konfigurieren** für die in der Liste ausgewählte Regel. Sie können die ausgewählte Regel ändern, indem Sie die Liste der Einträge in diesem Dialogfeld verwalten.
- **Nach oben** und **Nach unten** Ändern die Reihenfolge von Regeln in der Liste. Klicken Sie auf **Nach oben** oder **Nach unten**, um eine ausgewählte Regel in der Liste nach oben oder unten zu schieben, um also ihre Priorität zu erhöhen oder zu verringern.
- **Erweitert** Legen Sie bestimmte Optionen fest, die auf alle Regeln in der Liste angewandt werden, wie etwa die maximale Länge des generierten Namens, ob der Name nur aus Großbuchstaben oder aus Groß- und Kleinbuchstaben formatiert werden soll, den Bereich, in dem der generierte Name eindeutig sein soll, und die Zeichen, die aus den generierten Namen ausgeschlossen werden sollen.

Durch Aktivieren des Kontrollkästchens **Manuelle Bearbeitung von Anmeldenamen (Prä-Windows 2000) zulassen** autorisieren Sie den Operator, der das Benutzerkonto erstellt oder aktualisiert, zum Vornehmen von Änderungen an dem von der Richtlinie generierten Namen. Wenn dieses Kontrollkästchen deaktiviert ist, zeigt ActiveRoles Server in den Formularen zum Erstellen und Ändern von Benutzern das Feld **Benutzeranmeldename (Prä-Windows 2000)** schreibgeschützt an.

Durch Auswahl der Option **Immer** autorisieren Sie den Operator, den Prä-Windows 2000-Anmeldenamen nach Wunsch zu ändern. Mit der Option **Nur wenn durch diese Richtlinie ein eindeutiger Aliasname generiert werden kann** begrenzen Sie die manuellen Änderungen auf die Situation, in der kein eindeutiger Name in Übereinstimmung mit den Richtlinienregeln generiert werden kann.

Konfigurieren einer Generierungsrichtlinie für Anmeldenamen

Um eine Generierungsregel zu konfigurieren, klicken Sie unter der Liste **Generierungsregeln** auf die Schaltfläche **Hinzufügen**. Dann wird das Dialogfeld **Wert konfigurieren** angezeigt, in dem Sie aufgefordert werden, einen Wert für die Bedingung **„Anmeldename" muss sein** einzurichten.

Um mit dem Konfigurieren eines Wertes zu beginnen, klicken Sie im Dialogfeld **Wert konfigurieren** auf **Hinzufügen**. Nun wird das Fenster **Eintrag hinzufügen** angezeigt.

Ein Wert entsteht durch Verkettung von mindestens einem Eintrag. Im Fenster **Eintrag hinzufügen** können Sie den Typ des hinzuzufügenden Eintrags auswählen und den Eintrag dann konfigurieren. In der folgenden Tabelle werden die verfügbaren Eintragstypen zusammengefasst.

EINTRAGSTYP	BESCHREIBUNG
Text	Fügt dem Wert eine Textzeichenfolge hinzu.
Eindeutigkeitszahl	Fügt einen numerischen Wert hinzu, den die Richtlinie bei einem Namenskonflikt erhöhen soll.
Benutzereigenschaft	Fügt eine ausgewählte Eigenschaft (oder einen Teil einer Eigenschaft) des Benutzerkontos hinzu, dem die Richtlinie den Anmeldenamen zuweist.

EINTRAGSTYP	BESCHREIBUNG
Eigenschaft der übergeordneten Organisationseinheit	Fügt eine ausgewählte Eigenschaft (oder einen Teil einer Eigenschaft) einer Organisationseinheit in der Containerhierarchie über dem Benutzerkonto hinzu, dem die Richtlinie den Anmeldenamen zuweist.
Eigenschaft der übergeordneten Domäne	Fügt eine ausgewählte Eigenschaft (oder einen Teil einer Eigenschaft) der Domäne des Benutzerkontos hinzu, dem die Richtlinie den Anmeldenamen zuweist.

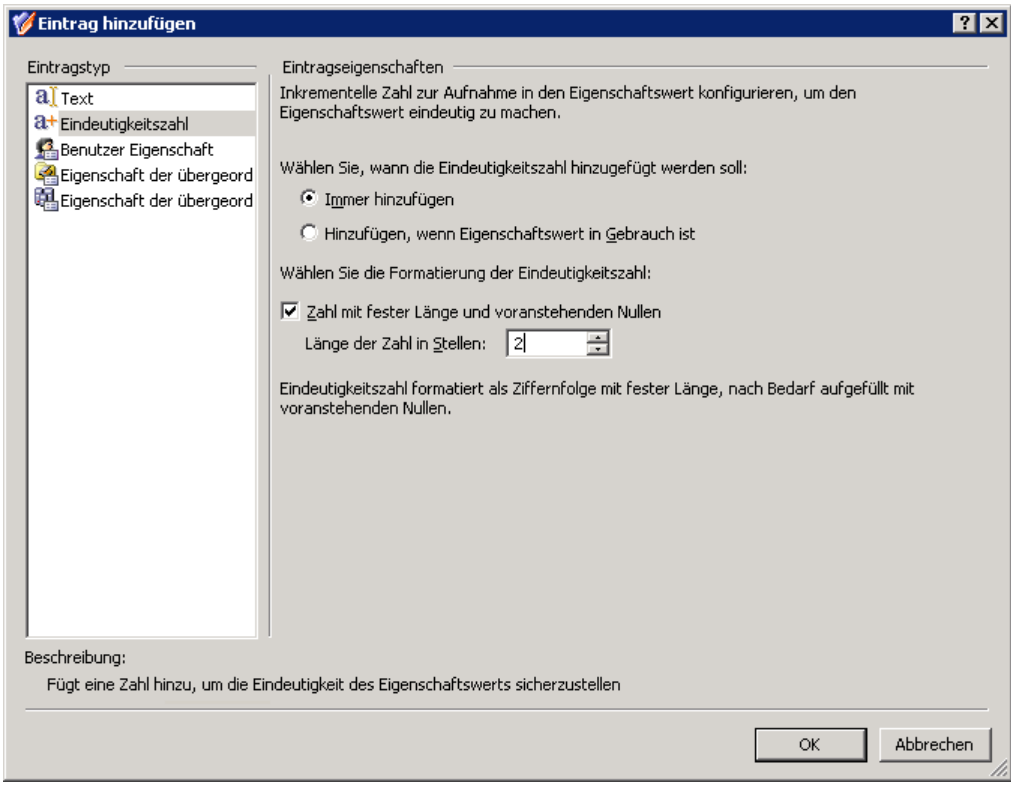
Die Anweisungen zum Konfigurieren eines Eintrags hängen vom Eintragstyp ab. Gehen Sie gemäß den Anweisungen vor, die im Abschnitt „Konfigurieren einer Richtlinie für die Generierung und Validierung von Eigenschaften" weiter oben in diesem Kapitel aufgeführt sind, um einen Eintrag eines dieser Typen zu konfigurieren:

- **Text** Siehe Unterabschnitt „Eintragstyp: Text".
- **Benutzereigenschaft** Siehe Unterabschnitt „Eintragstyp: <Objekt> Eigenschaft".
- **Eigenschaft der übergeordneten Organisationseinheit** Siehe Unterabschnitt „Eintragstyp: Eigenschaft der übergeordneten Organisationseinheit".
- **Eigenschaft der übergeordneten Domäne** Siehe Unterabschnitt „Eintragstyp: Eigenschaft der übergeordneten Domäne".

Im folgenden Unterabschnitt wird der Eintrag **Eindeutigkeitszahl** erörtert.

Eintragstyp: Eindeutigkeitszahl

Wenn Sie im Fenster **Eintrag hinzufügen** unter **Eintragstyp** den Typ **Eindeutigkeitszahl** auswählen, ähnelt der Bereich **Eintragseigenschaften** der folgenden Abbildung.


Eintrag hinzufügen
Eintragstyp
Text
Eindeutigkeitszahl
Benutzer Eigenschaft
Eigenschaft der übergeord
Eigenschaft der übergeord
Eintragseigenschaften
Inkrementelle Zahl zur Aufnahme in den Eigenschaftswert konfigurieren, um den Eigenschaftswert eindeutig zu machen.
Wählen Sie, wann die Eindeutigkeitszahl hinzugefügt werden soll:
Immer hinzufügen
Hinzufügen, wenn Eigenschaftswert in Gebrauch ist
Wählen Sie die Formatierung der Eindeutigkeitszahl:
Zahl mit fester Länge und voranstehenden Nullen
Länge der Zahl in Stellen:
2
Eindeutigkeitszahl formatiert als Ziffernfolge mit fester Länge, nach Bedarf aufgefüllt mit voranstehenden Nullen.
Beschreibung:
Fügt eine Zahl hinzu, um die Eindeutigkeit des Eigenschaftswerts sicherzustellen
OK
Abbrechen

Mit diesem Eintragstyp können Sie einen Eintrag hinzufügen, der eine Zahl darstellt, den die Richtlinie im Fall eines Namenskonflikts erhöht.

Sie müssen zuerst auswählen, wann die Richtlinie diesen Eintrag verwenden soll. Folgende Optionen stehen zur Verfügung:

- **Immer hinzufügen** Der Wert schließt diesen Eintrag unabhängig davon ein, ob die Richtlinie bei der Anwendung der Generierungsregel einen Namenskonflikt erkennt.
- **Hinzufügen, wenn Eigenschaftswert in Gebrauch ist** Die Richtlinie fügt diesen Eintrag bei einem Namenskonflikt zum Wert hinzu; ansonsten enthält dieser Wert nicht diesen Eintrag.

Als Nächstes können Sie angeben, wie der Eintrag formatiert werden soll:

- Damit er als Ziffernfolge variabler Länge formatiert wird, deaktivieren Sie das Kontrollkästchen **Zahl mit fester Länge und voranstehenden Nullen**. In den meisten Fällen ergibt dies einen Eintrag aus nur einer Ziffer.
- Damit der Eintrag als Ziffernfolge fester Länge formatiert wird, aktivieren Sie das Kontrollkästchen **Zahl mit fester Länge und voranstehenden Nullen**, und geben Sie dann die gewünschte Ziffernanzahl ein. Dies generiert einen Eintrag mit der passenden Anzahl von Nullen als Präfix, z.B. 001, 002, 003.

Klicken Sie nach dem Konfigurieren eines Eintrags auf **OK**, um das Fenster **Eintrag hinzufügen** zu schließen. Der Eintrag wird dem Dialogfeld **Wert konfigurieren** hinzugefügt.

Klicken Sie nach dem Konfigurieren eines Wertes auf **OK**, um das Dialogfeld **Wert konfigurieren** zu schließen. Dann wird die Regel zu der Liste auf der Seite **Regeln zur Generierung von Benutzeranmeldenamen (Prä-Windows 2000)** hinzugefügt.

Klicken Sie nach dem Konfigurieren der Richtlinienregeln auf der Seite **Regeln zur Generierung von Benutzeranmeldenamen (Prä-Windows 2000)** auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schrittweise Anleitungen finden Sie unter **Anleitungen/Verwalten von Richtlinienobjekten/ Konfigurieren von Bereitstellungsrichtlinienobjekten/Konfigurieren einer Richtlinie zur Generierung eines Benutzeranmeldenamens** in der ActiveRoles Server-Hilfe.

Szenario 1: Verwenden einer Eindeutigkeitszahl

Die in diesem Szenario beschriebene Richtlinie generiert den Benutzer-Anmeldenamen (Prä-Windows 2000) in Übereinstimmung mit folgender Regel: das erste Zeichen des Vornamens des Benutzers, dann optional eine Eindeutigkeitszahl, dann der Nachname des Benutzers. Der von der Richtlinie generierte Name ist höchstens 8 Zeichen lang. Wenn der Name länger ist, werden die hinteren Zeichen bei Bedarf abgeschnitten. Es folgen Beispiele für Namen, die von dieser Richtlinie generiert werden:

- JSmitson
- J1Smitso
- J2Smitso

Die Richtlinie generiert den Namen J1Smitso für den Benutzer John Smitson, falls der Name JSmitson bereits verwendet wird. Wenn JSmitson und J1Smitso schon verwendet werden, generiert die Richtlinie den Namen J2Smitso usw.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen und konfigurieren Sie das Richtlinienobjekt, das die entsprechende Richtlinie definiert.
2. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Wenn Sie nun einem Benutzerkonto in dem in Schritt 2 ausgewählten Container einen Benutzer-Anmeldenamen (Prä-Windows 2000) zuweisen, stellen die Benutzeroberflächen von ActiveRoles Server die Schaltfläche **Generieren** bereit, mit der ein Name in Übereinstimmung mit der Richtlinienregel erstellt werden kann. Wenn Sie im Fall eines Namenskonflikts auf die Schaltfläche **Generieren** klicken, fügt die Richtlinie dem Namen eine Eindeutigkeitszahl hinzu.

In den folgenden beiden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen und Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt mit dem Assistenten für neues Bereitstellungsrichtlinienobjekt erstellen und konfigurieren. Weitere Informationen über den Assistenten finden Sie unter „Erstellen eines Richtlinienobjekts" im Abschnitt „Verwaltungsaufgaben für Richtlinienobjekte" weiter oben in diesem Kapitel.

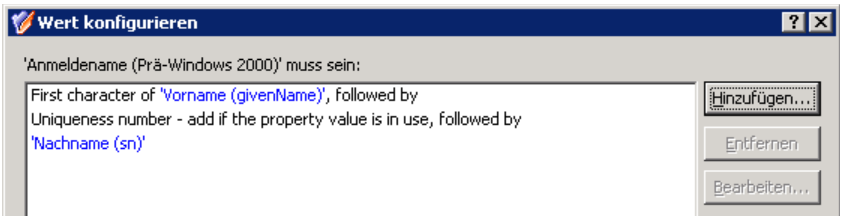
Klicken Sie zum Konfigurieren der Richtlinie auf der Seite **Richtlinientyp auswählen** des Assistenten auf **Erzeugung von Benutzeranmeldenamen**. Klicken Sie dann auf **Weiter**.

Klicken Sie auf der Seite **Regeln zur Generierung von Benutzeranmeldenamen (Prä-Windows 2000)** auf **Hinzufügen**. Füllen Sie dann das Dialogfeld **Wert konfigurieren** wie folgt aus:

1. Klicken Sie auf **Hinzufügen**.
2. Konfigurieren Sie den Eintrag so, dass das erste Zeichen des Vornamens des Benutzers eingeschlossen wird:
   a) Klicken Sie unter **Eintragstyp** auf **Benutzereigenschaft**.
   b) Klicken Sie unter **Eintragseigenschaften** auf **Auswählen**.
   c) Klicken Sie im Fenster **Objekteigenschaft wählen** auf **Vorname** in der Liste **Objekteigenschaft** und klicken Sie dann auf **OK**.
   d) Klicken Sie unter **Eintragseigenschaften** auf **Die ersten**, und stellen Sie sicher, dass das Feld neben dieser Option den Wert **1** enthält.
   e) Klicken Sie auf **OK**.
3. Klicken Sie auf **Hinzufügen**.
4. Konfigurieren Sie wie folgt den Eintrag so, dass er optional eine Eindeutigkeitszahl enthält:
   a) Klicken Sie unter **Eintragstyp** auf **Eindeutigkeitszahl**.
   b) Klicken Sie unter **Eintragseigenschaften** auf **Hinzufügen, wenn Eigenschaftswert in Gebrauch ist**, und stellen Sie sicher, dass das Kontrollkästchen **Zahl mit fester Länge und voranstehenden Nullen** deaktiviert ist.
   c) Klicken Sie auf **OK**.
5. Klicken Sie auf **Hinzufügen**.

6. Konfigurieren Sie den Eintrag so, dass er den Nachnamen des Benutzers enthält:
   a) Klicken Sie unter **Eintragstyp** auf **Benutzereigenschaft**.
   b) Klicken Sie unter **Eintragseigenschaften** auf **Auswählen**.
   c) Klicken Sie im Fenster **Objekteigenschaft wählen** auf **Nachname** in der Liste **Objekteigenschaft** und klicken Sie dann auf **OK**.
   d) Klicken Sie auf **OK**.

Nach dem Ausführen dieser Schritte sollte die Liste der Einträge im Dialogfeld **Wert konfigurieren** der folgenden Abbildung ähneln.


Wert konfigurieren
'Anmeldename (Prä-Windows 2000)' muss sein:
First character of 'Vorname (givenName)', followed by
Uniqueness number - add if the property value is in use, followed by
'Nachname (sn)'
Hinzufügen...
Entfernen
Bearbeiten...

Klicken Sie auf **OK**, um das Dialogfeld **Wert konfigurieren** zu schließen.

Richten Sie nun die Grenze für die Namenslänge ein. Klicken Sie auf der Seite **Regeln zur Generierung von Benutzeranmeldenamen (Prä-Windows 2000)** auf die Schaltfläche **Erweitert**. Geben Sie im Dialogfeld **Erweitert** in das Feld **Maximale Länge in Zeichen** den Wert **8** ein und klicken Sie dann auf **OK**.

Klicken Sie auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schritt 2: Anwenden des Richtlinienobjekts

Sie können das Richtlinienobjekt mit Hilfe der Seite **Richtlinie erzwingen** im Assistenten für neues Bereitstellungsrichtlinienobjekt anwenden oder Sie können den Assistenten erst abschließen und dann den Befehl **Richtlinie erzwingen** für die Domäne, die Organisationseinheit oder die verwaltete Einheit verwenden, auf die Sie die Richtlinie anwenden möchten.

Weitere Informationen über die Anwendung eines Richtlinienobjekts finden Sie unter „Anwenden von Richtlinienobjekten“ und „Verwalten des Richtlinienbereichs“ weiter oben in diesem Kapitel.

Szenario 2: Verwenden mehrerer Regeln

Die in diesem Szenario beschriebene Richtlinie verwendet mehrere Regeln, um den Benutzer-Anmeldenamen (Prä-Windows 2000) zu generieren. Die Regeln lauten wie folgt:

1. Das erste Zeichen des Vornamens des Benutzers, gefolgt vom Nachnamen des Benutzers
2. Die ersten beiden Zeichen des Vornamens des Benutzers, gefolgt vom Nachnamen des Benutzers
3. Die ersten drei Zeichen des Vornamens des Benutzers, gefolgt vom Nachnamen des Benutzers

Der von der Richtlinie generierte Name ist höchstens 8 Zeichen lang. Wenn der Name länger ist, werden die hinteren Zeichen bei Bedarf abgeschnitten.

Es folgen Beispiele für Namen, die von dieser Richtlinie generiert werden:

- JSmitson
- JoSmitso
- JohSmits

Die Richtlinie generiert den Namen JoSmitso für den Benutzer John Smitson, falls der Name JSmitson bereits verwendet wird. Wenn JSmitson und JoSmitso schon verwendet werden, generiert die Richtlinie den Namen JohSmits.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Konfigurieren Sie das Richtlinienobjekt, das die entsprechende Richtlinie definiert.
2. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Wenn Sie nun einem Benutzerkonto in dem in Schritt 2 ausgewählten Container einen Benutzer-Anmeldenamen (Prä-Windows 2000) zuweisen, stellen die Benutzeroberflächen von ActiveRoles Server die Schaltfläche **Generieren** bereit, mit der der Name in Übereinstimmung mit den Richtlinienregeln erstellt werden kann. Wenn Sie im Fall eines Namenskonflikts auf die Schaltfläche **Generieren** klicken, verwendet die Richtlinie eine der folgenden Regeln.

In den folgenden beiden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

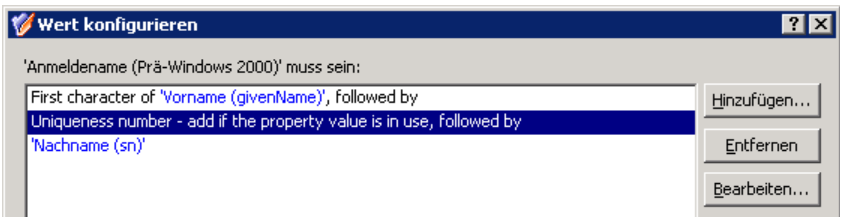
Schritt 1: Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt konfigurieren, indem Sie das Richtlinienobjekt ändern, das das vorige Szenario implementiert; siehe „Szenario 1: Verwenden einer Eindeutigkeitszahl" weiter oben in diesem Abschnitt.

Zeigen Sie das Dialogfeld **Eigenschaften** für dieses Richtlinienobjekt an und öffnen Sie die Registerkarte **Richtlinien**. Wählen Sie dann in der Liste die Richtlinie aus, und klicken Sie auf **Anzeigen/Bearbeiten**, um das Dialogfeld **Eigenschaften der Benutzeranmeldenamen-Generierungsrichtlinie** anzuzeigen.

Die Registerkarte **Generierungsregeln** im Dialogfeld **Eigenschaften der Benutzeranmeldenamen-Generierungsrichtlinie** ähnelt der Seite **Regeln zur Generierung von Benutzeranmeldenamen (Prä-Windows 2000)** des Assistenten, mit dem Sie die Richtlinie konfiguriert haben. Auf dieser Registerkarte können Sie Richtlinienregeln hinzufügen oder ändern.

Ändern Sie die Regel zunächst, indem Sie den Eintrag für die Eindeutigkeitszahl entfernen. Wählen Sie auf der Registerkarte **Generierungsregeln** die Regel aus, und klicken Sie auf **Anzeigen/Bearbeiten**, um das Dialogfeld **Wert konfigurieren** anzuzeigen. Wählen Sie dann den Eindeutigkeitszahleintrag aus, wie in der folgenden Abbildung gezeigt, und klicken Sie auf **Entfernen**.

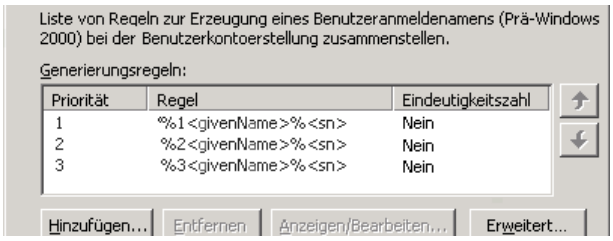

Wert konfigurieren
'Anmeldename (Prä-Windows 2000)' muss sein:
First character of 'Vorname (givenName)', followed by
Uniqueness number - add if the property value is in use, followed by
'Nachname (sn)'
Hinzufügen...
Entfernen
Bearbeiten...

Klicken Sie auf **OK**, um das Dialogfeld **Wert konfigurieren** zu schließen.

Konfigurieren Sie nun wie folgt die zusätzlichen Richtlinienregeln:

1. Klicken Sie auf der Registerkarte **Generierungsregeln** auf **Hinzufügen**, um das Dialogfeld **Wert konfigurieren** anzuzeigen.
2. Klicken Sie im Dialogfeld **Wert konfigurieren** auf **Hinzufügen**, um das Fenster **Eintrag hinzufügen** anzuzeigen.
3. Konfigurieren Sie den Eintrag so, dass die ersten beiden Zeichen des Vornamens des Benutzers eingeschlossen wird:
   a) Klicken Sie unter **Eintragstyp** auf **Benutzereigenschaft**.
   b) Klicken Sie unter **Eintragseigenschaften** auf **Auswählen**.
   c) Klicken Sie im Fenster **Objekteigenschaft wählen** auf **Vorname** in der Liste **Objekteigenschaft** und klicken Sie dann auf **OK**.
   d) Klicken Sie unter **Eintragseigenschaften** auf **Die ersten** und geben Sie in das Feld neben dieser Option den Wert **2** ein.
   e) Klicken Sie auf **OK**, um das Fenster **Eintrag hinzufügen** zu schließen.
4. Klicken Sie im Dialogfeld **Wert konfigurieren** auf **Hinzufügen**, um das Fenster **Eintrag hinzufügen** anzuzeigen.
5. Konfigurieren Sie den Eintrag so, dass er den Nachnamen des Benutzers enthält:
   a) Klicken Sie unter **Eintragstyp** auf **Benutzereigenschaft**.
   b) Klicken Sie unter **Eintragseigenschaften** auf **Auswählen**.
   c) Klicken Sie im Fenster **Objekteigenschaft wählen** auf **Nachname** in der Liste **Objekteigenschaft** und klicken Sie dann auf **OK**.
   d) Klicken Sie auf **OK**, um das Fenster **Eintrag hinzufügen** zu schließen.
6. Klicken Sie auf **OK**, um das Dialogfeld **Wert konfigurieren** zu schließen.
7. Wiederholen Sie die Schritte 1 bis 6 mit folgender Abweichung:
   Geben Sie in Schritt 3 im Teilschritt d) in das Feld neben der Option **Die ersten** den Wert **3** ein.

Nach der Ausführung dieser Schritte sollte die Liste der Regeln auf der Registerkarte **Generierungsregeln** folgendes Aussehen aufweisen:



Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften der Benutzeranmeldenamen-Generierungsrichtlinie** zu schließen.

Schritt 2: Anwenden des Richtlinienobjekts

Um das Richtlinienobjekt anzuwenden, können Sie im Dialogfeld **Eigenschaften** für dieses Richtlinienobjekt die Registerkarte **Bereich** verwenden:

1. Klicken Sie auf der Registerkarte **Bereich** auf die Schaltfläche **Bereich**, um das Fenster **ActiveRoles Serverrichtlinienbereich** für das zu verwaltende Richtlinienobjekt anzuzeigen.
2. Klicken Sie auf **Hinzufügen** und wählen Sie die Domäne, Organisationseinheit oder verwaltete Einheit aus, auf die Sie die Richtlinie anwenden möchten.

   *Sie können auch mit Hilfe der Schaltfläche **Entfernen** Elemente entfernen, auf die die Richtlinie nicht mehr angewendet werden soll.*
3. Klicken Sie auf **OK**, um das Fenster **ActiveRoles Serverrichtlinienbereich** zu schließen.
4. Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften** für das Richtlinienobjekt zu schließen.

Weitere Informationen über die Anwendung eines Richtlinienobjekts finden Sie unter „Anwenden von Richtlinienobjekten" und „Verwalten des Richtlinienbereichs" weiter oben in diesem Kapitel.

Automatische Bereitstellung der Gruppenmitgliedschaft

Richtlinien dieser Kategorie dienen zum Automatisieren des Hinzufügens oder Entfernens angegebener Objekte wie z.B. Benutzerobjekte in angegebenen Gruppen.

Sie können Objekttypen sowie Gruppen auswählen und Richtlinienregeln einrichten. Die Richtlinie fügt den ausgewählten Gruppen Objekte hinzu oder entfernt sie daraus, je nachdem, ob diese Objekte den angegebenen Regeln entsprechen.

Funktionsweise dieser Richtlinie

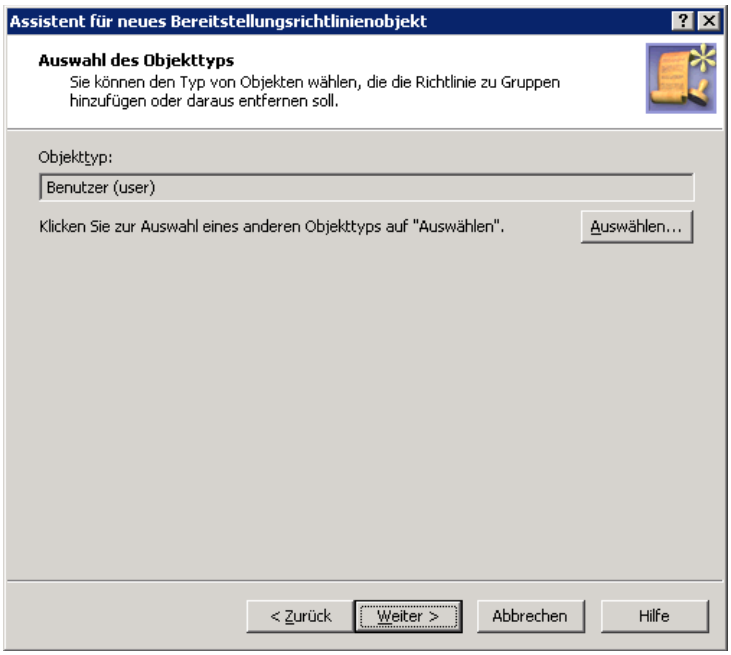
Die Richtlinie „Automatische Bereitstellung der Gruppenmitgliedschaft" für die Gruppenmitgliedschaft führt Bereitstellungsaufgaben aus, wie das Hinzufügen oder Entfernen von Benutzern in Gruppen. Eine Richtlinie kann so konfiguriert werden, dass sie eine Liste von Gruppen und Bedingungen definiert, wobei den Gruppen ein Benutzerkonto automatisch hinzugefügt bzw. aus ihnen entfernt wird, je nachdem, ob die Eigenschaften des Benutzerkontos die Richtlinienbedingungen erfüllen.

ActiveRoles Server überprüft Benutzer automatisch anhand von Bedingungen und fügt die Benutzer basierend auf den Überprüfungsergebnissen angegebenen Gruppen hinzu oder entfernt sie aus diesen. Zwar ähneln die Funktionen dieser Richtlinie denen dynamischer Gruppen; die Richtlinie „Automatische Bereitstellung der Gruppenmitgliedschaft" ermöglicht dem Administrator jedoch zusätzliche Flexibilität und Kontrolle über Gruppenmitgliedschaften.

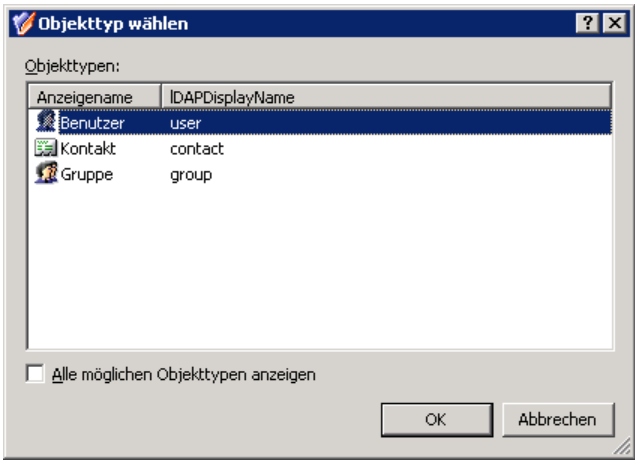
Während die Funktion für dynamische Gruppen einen regelorientierten Verwaltungsmechanismus für die Verwaltung der gesamten Gruppenmitgliedschaftsliste bietet, ermöglicht die Richtlinie „Automatische Bereitstellung der Gruppenmitgliedschaft" dem Administrator das Definieren von Mitgliedschaftsregeln für einzelne Benutzer. Diese Richtlinie automatisiert das Hinzufügen bestimmter Benutzer zu bestimmten Gruppen ohne Auswirkungen auf die anderen Mitglieder dieser Gruppen.

Konfigurieren der Richtlinie „Automatische Bereitstellung der Gruppenmitgliedschaft"

Um die Richtlinie „Automatische Bereitstellung der Gruppenmitgliedschaft" zu konfigurieren, wählen Sie **Automatische Bereitstellung der Gruppenmitgliedschaft** auf der Seite **Zu konfigurierende Richtlinie** im Assistenten für neues Bereitstellungsrichtlinienobjekt oder im Assistenten „Bereitstellungsrichtlinie hinzufügen" aus. Klicken Sie dann auf **Weiter**, damit die Seite **Auswahl des Objekttyps** angezeigt wird.

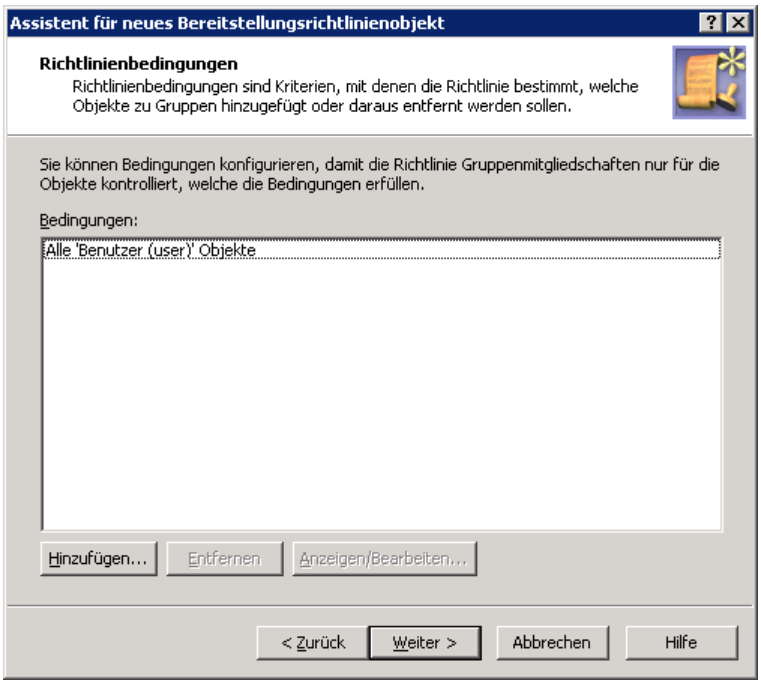

Assistent für neues Bereitstellungsrichtlinienobjekt
Auswahl des Objekttyps
Sie können den Typ von Objekten wählen, die die Richtlinie zu Gruppen hinzufügen oder daraus entfernen soll.
Objekttyp:
Benutzer (user)
Klicken Sie zur Auswahl eines anderen Objekttyps auf "Auswählen".
Auswählen...
< Zurück
Weiter >
Abbrechen
Hilfe

Auf dieser Seite können Sie den Typ von Objekten auswählen, die die Richtlinie zu Gruppen hinzufügen oder aus ihnen entfernen soll. Standardmäßig ist der Objekttyp auf Benutzer festgelegt. Wenn Sie diese Einstellung ändern möchten, klicken Sie auf **Auswählen**, um das Dialogfeld **Objekttyp wählen** anzuzeigen.



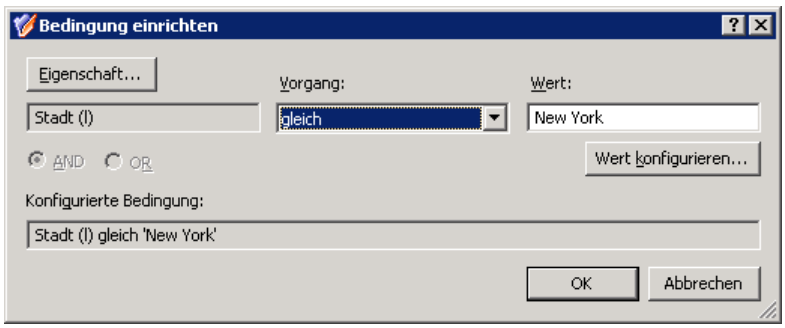
Wählen Sie in der Liste **Objekttypen** den Typ der Objekte aus, die die Richtlinie steuern soll. Klicken Sie auf **OK**.

Klicken Sie auf der Seite **Auswahl des Objekttyps** auf **Weiter**, um die Seite **Richtlinienbedingungen** anzuzeigen.


Assistent für neues Bereitstellungsrichtlinienobjekt
Richtlinienbedingungen
Richtlinienbedingungen sind Kriterien, mit denen die Richtlinie bestimmt, welche Objekte zu Gruppen hinzugefügt oder daraus entfernt werden sollen.
Sie können Bedingungen konfigurieren, damit die Richtlinie Gruppenmitgliedschaften nur für die Objekte kontrolliert, welche die Bedingungen erfüllen.
Bedingungen:
Alle 'Benutzer (user)' Objekte
Hinzufügen...
Entfernen
Anzeigen/Bearbeiten...
< Zurück
Weiter >
Abbrechen
Hilfe

Auf dieser Seite können Sie Richtlinienbedingungen einrichten, also Kriterien, mit denen die Richtlinie bestimmt, welche Objekte zu Gruppen hinzugefügt bzw. aus ihnen entfernt werden. Wenn Sie keine Bedingungen angeben, wirkt sich die Richtlinie auf alle Objekte des auf der vorigen Seite ausgewählten Typs aus. Wenn Sie auf dieser Seite Bedingungen angeben, wirkt sie sich nur auf die Objekte aus, die sie erfüllen.

Klicken Sie zum Konfigurieren einer Bedingung auf der Seite **Richtlinienbedingungen** auf **Hinzufügen**. Nun wird das Dialogfeld **Bedingung einrichten** angezeigt.



In diesem Dialogfeld können Sie eine Bedingung auf die gleiche Weise konfigurieren wie für eine Richtlinie „Erzeugung und Validierung von Eigenschaften". Eine Bedingung enthält eine Objekteigenschaft (beispielsweise **Stadt** oder **Department**), eine Anforderung (beispielsweise **gleich** oder **beginnt mit**) und einen Wert. Der Begriff *Wert* hat dieselbe Bedeutung wie für die Richtlinie „Erzeugung und Validierung von Eigenschaften".

Klicken Sie zuerst auf die Schaltfläche **Eigenschaft**, um das Dialogfeld **Objekteigenschaft wählen** anzuzeigen, in dem Sie die Objekteigenschaft auswählen können, die in die Bedingung eingeschlossen werden soll.

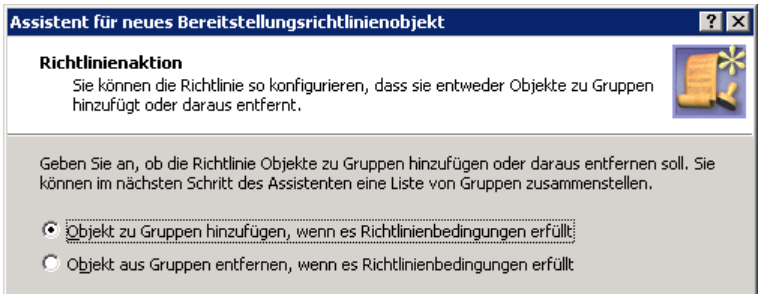
Wählen Sie dann in der Liste **Vorgang** die Anforderung aus, die Sie auf die ausgewählte Eigenschaft anwenden möchten.

Klicken Sie nun auf die Schaltfläche **Wert konfigurieren**, um den Wert einzurichten, auf den Sie die ausgewählte Anforderung anwenden möchten. Hierdurch wird das Dialogfeld **Wert konfigurieren** geöffnet, das weiter oben in diesem Kapitel beschrieben wurde (siehe „Konfigurieren einer Richtlinie für die Generierung und Validierung von Eigenschaften"). In diesem Dialogfeld können Sie einen Wert auf die gleiche Weise einrichten wie für die Richtlinie „Erzeugung und Validierung von Eigenschaften".

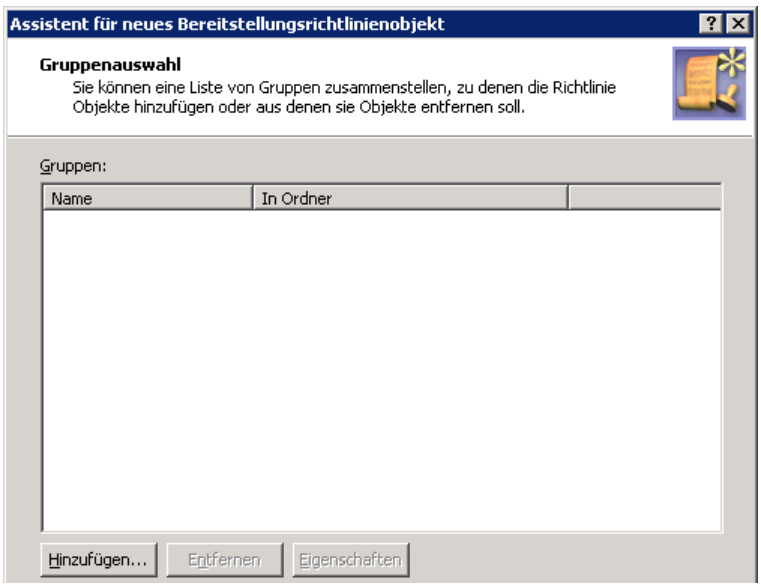
Wenn Sie mehrere Bedingungen angeben, können Sie sie mit dem logischen Operator UND oder ODER kombinieren, indem Sie auf die Option **UND** bzw. **ODER** klicken.

Klicken Sie abschließend auf **OK**, um das Dialogfeld **Bedingung einrichten** zu schließen.

Wenn Sie die Liste auf der Seite **Richtlinienbedingungen** fertig gestellt haben, klicken Sie auf **Weiter**, um die Seite **Richtlinienaktion** anzuzeigen:


Assistent für neues Bereitstellungsrichtlinienobjekt
Richtlinienaktion
Sie können die Richtlinie so konfigurieren, dass sie entweder Objekte zu Gruppen hinzufügt oder daraus entfernt.
Geben Sie an, ob die Richtlinie Objekte zu Gruppen hinzufügen oder daraus entfernen soll. Sie können im nächsten Schritt des Assistenten eine Liste von Gruppen zusammenstellen.
Objekt zu Gruppen hinzufügen, wenn es Richtlinienbedingungen erfüllt
Objekt aus Gruppen entfernen, wenn es Richtlinienbedingungen erfüllt

Auf dieser Seite können Sie die Richtlinie so konfigurieren, dass Sie Objekte zu Gruppen hinzufügt oder aus ihnen entfernt. Wenn Sie beispielsweise die Option **Objekt zu Gruppen hinzufügen, wenn es Richtlinienbedingungen erfüllt** auswählen, füllt die Richtlinie Gruppen mit den Objekten auf, die die im vorigen Schritt eingerichteten Bedingungen erfüllen. Klicken Sie auf **Weiter**, um die Gruppen anzugeben, die die Richtlinie auffüllen soll. Hierdurch wird die Seite **Gruppenauswahl** angezeigt.



Auf der Seite **Gruppenauswahl** können Sie eine Liste von Gruppen einrichten, die von der Richtlinie gesteuert werden sollen. Abhängig von der im vorigen Schritt ausgewählten Option fügt die Richtlinie jeder auf dieser Seite angegebenen Gruppe Objekte hinzu oder entfernt Objekte aus ihr. Sie können die Liste mit Hilfe der Schaltflächen **Hinzufügen** und **Entfernen** verwalten. Wenn Sie auf **Hinzufügen** klicken, wird das Dialogfeld **Objekte auswählen** angezeigt, mit dem Sie Gruppen auswählen und der Liste hinzufügen können. Wenn Sie auf **Entfernen** klicken, werden die ausgewählten Einträge aus der Liste gelöscht.

Klicken Sie nach dem Einrichten der Gruppenliste auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schrittweise Anleitungen finden Sie unter **Anleitungen/Verwalten von Richtlinienobjekten/ Konfigurieren von Bereitstellungsrichtlinienobjekten/Konfigurieren einer Richtlinie zur automatischen Bereitstellung von Gruppenmitgliedschaften** in der ActiveRoles Server-Hilfe.

Szenario: Hinzufügen von Benutzern zu einer angegebenen Gruppe

Die in diesem Szenario beschriebene Richtlinie fügt automatisch Benutzerkonten den angegebenen Gruppen hinzu, in Abhängigkeit von der Eigenschaft der **Department** Benutzerkonten. Wenn die Eigenschaft **Department** eines Benutzerkontos auf **Vertrieb** festgelegt ist, fügt die Richtlinie das Konto der Gruppe **Vertrieb** hinzu.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen und konfigurieren Sie ein Richtlinienobjekt, das die entsprechende Richtlinie definiert.
2. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Wenn für ein Benutzerkonto in dem in Schritt 2 ausgewählten Container die Eigenschaft **Department** auf **Vertrieb** festgelegt ist, fügt ActiveRoles Server das Konto folglich automatisch der Gruppe **Vertrieb** hinzu.

In den folgenden beiden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen und Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt mit dem Assistenten für neues Bereitstellungsrichtlinien-objekt erstellen und konfigurieren. Weitere Informationen über den Assistenten finden Sie unter „Erstellen eines Richtlinienobjekts" im Abschnitt „Verwaltungsaufgaben für Richtlinienobjekte" weiter oben in diesem Kapitel.

Klicken Sie zum Konfigurieren der Richtlinie auf der Seite **Richtlinientyp auswählen** des Assistenten auf **Automatische Bereitstellung der Gruppenmitgliedschaft**. Klicken Sie dann auf **Weiter**.

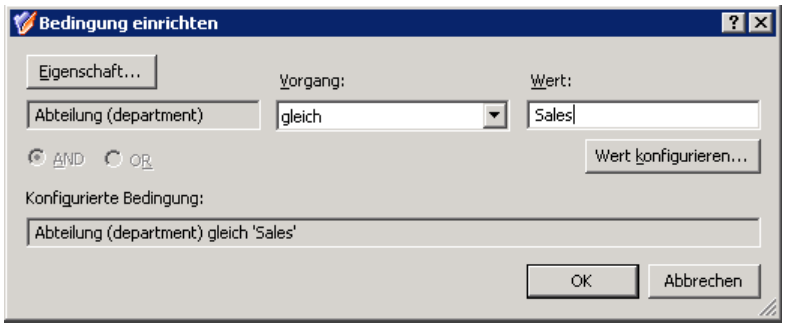
Klicken Sie auf der Seite **Auswahl des Objekttyps** auf **Weiter**, um die Standardeinstellung zu akzeptieren, also den Objekttyp für Benutzer.

Klicken Sie auf der Seite **Richtlinienbedingungen** auf **Hinzufügen**, um das Dialogfeld **Bedingung einrichten** anzuzeigen.

Konfigurieren Sie die Bedingung wie folgt:

1. Klicken Sie auf die Schaltfläche **Eigenschaft**; aktivieren Sie dann das Kontrollkästchen **Abteilung** und klicken Sie anschließend auf **OK**.
2. Geben Sie in das Feld **Wert** den Wert **Vertrieb** ein.

Nach der Ausführung dieser Schritte entspricht das Dialogfeld **Bedingung einrichten** der folgenden Abbildung.



Klicken Sie auf **OK**, um das Dialogfeld **Bedingung einrichten** zu schließen.

Klicken Sie auf der Seite **Richtlinienbedingungen** auf **Weiter**.

Klicken Sie auf der Seite **Richtlinienaktion** auf **Objekt zu Gruppen hinzufügen, wenn es Richtlinienbedingungen erfüllt** und klicken Sie dann auf **Weiter**.

Klicken Sie auf der Seite **Gruppenauswahl** auf **Hinzufügen** und suchen Sie dann im Dialogfeld **Objekte auswählen** die Gruppe **Vertrieb**. Wenn Sie die Gruppe **Vertrieb** zu der Liste auf der Seite **Gruppenauswahl** hinzugefügt haben, klicken Sie auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schritt 2: Anwenden des Richtlinienobjekts

Sie können das Richtlinienobjekt mit Hilfe der Seite **Richtlinie erzwingen** im Assistenten für neues Bereitstellungsrichtlinienobjekt anwenden oder Sie können den Assistenten erst abschließen und dann den Befehl **Richtlinie erzwingen** für die Domäne, die Organisationseinheit oder die verwaltete Einheit verwenden, auf die Sie die Richtlinie anwenden möchten.

Weitere Informationen über die Anwendung eines Richtlinienobjekts finden Sie unter „Anwenden von Richtlinienobjekten“ und „Verwalten des Richtlinienbereichs“ weiter oben in diesem Kapitel.

E-Mail-Aliaserzeugung

Richtlinien dieser Kategorie dienen zum Automatisieren der Zuweisung des E-Mail-Alias, wenn ein Benutzer in Microsoft Exchange Server für die Verwendung von Postfächern aktiviert wird. Standardmäßig stellt Microsoft Exchange Server das folgende Format für E-Mail-Adressen von Empfängern bereit: *<E-Mail-Alias>*@*<Domänenname>*

Sie können E-Mail-Aliase mittels vordefinierter Regeln generieren oder benutzerdefinierte Regeln konfigurieren. Sie können beispielsweise eine Richtlinie konfigurieren, mit der der E-Mail-Alias aus dem Anfangsbuchstaben des Vornamens und dem Nachnamen des Benutzers zusammengestellt wird. Mit Hilfe benutzerdefinierter Regeln können Sie einen inkrementellen numerischen Wert hinzufügen, um die Eindeutigkeit des Alias sicherzustellen. Sie können auch angeben, ob der Alias von dem Operator geändert werden kann, der das Benutzerkonto erstellt oder aktualisiert.

Funktionsweise dieser Richtlinie

Wenn ein Benutzer für die Verwendung von Postfächern aktiviert wird, verwendet ActiveRoles Server diese Richtlinie, um dem Benutzerkonto einen bestimmten E-Mail-Alias zuzuweisen. Die Richtlinie generiert den Alias basierend auf Benutzereigenschaften, z.B. dem Benutzer-Anmeldenamen (Prä-Windows 2000), dem Vornamen, den Initialen und dem Nachnamen. Zum Verwenden anderer Eigenschaften kann eine benutzerdefinierte Regel konfiguriert werden.

Außerdem kann eine benutzerdefinierte Regel konfiguriert werden, um eine so genannte *Eindeutigkeitszahl* hinzuzufügen. Die Eindeutigkeitszahl ist ein numerischer Wert, den die Richtlinie in den Alias einschließt und den sie bei einem Aliasnamenskonflikt erhöht. Die Richtlinie kann beispielsweise automatisch den generierten Alias von John.Smith in John1.Smith ändern, wenn bereits ein Postfach mit dem Alias John.Smith vorhanden ist. Wenn auch der Alias John1.Smith bereits verwendet wird, wird der neue Alias in John2.Smith geändert und so weiter.

Bei der Richtlinienkonfiguration besteht die Option, die manuelle Bearbeitung von Aliasen, die durch Richtlinien generiert wurden, zuzulassen oder zu verweigern. Die Berechtigung zum Ändern eines Alias, der durch eine Richtlinie generiert wurde, kann auf den Fall eingeschränkt werden, dass der Alias von einem anderen Postfach verwendet wird.

Es folgen einige spezifische Aspekte des Richtlinienverhaltens:

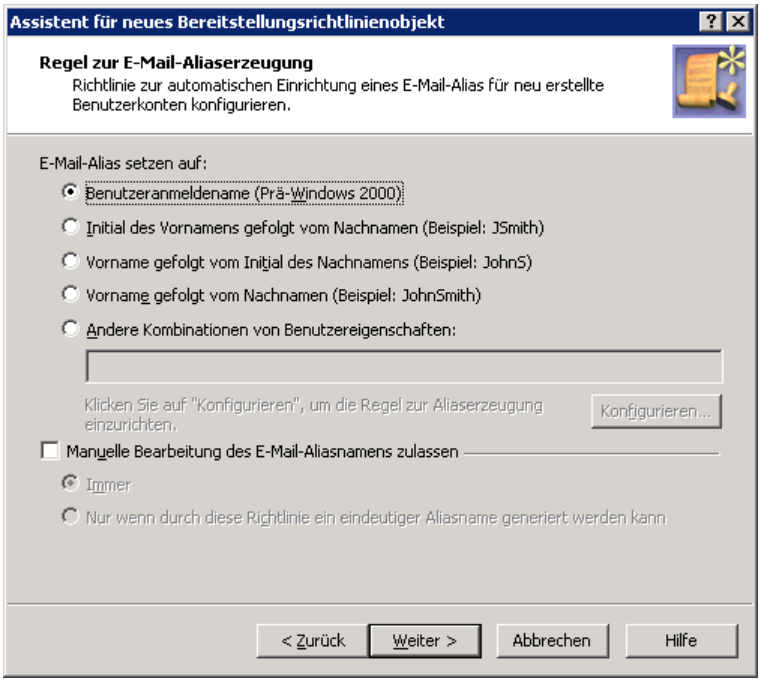
- Mit einer Regel, die keine Eindeutigkeitszahl verwendet, versucht ActiveRoles Server einfach, dem Benutzerkonto den generierten Alias zuzuweisen. Dieser Vorgang kann fehlschlagen, wenn der generierte Alias nicht eindeutig ist, wenn er also schon einem anderen Benutzerkonto zugewiesen wurde. Wenn die Richtlinie die manuelle Bearbeitung von Aliasen zulässt, die sie generiert hat, kann der Alias von dem Operator korrigiert werden, der das Benutzerkonto erstellt.
- Wenn eine benutzerdefinierte Regel mit Eindeutigkeitszahlen vorliegen, wird in ActiveRoles Server auf der Clientseite auf den Formularen für die Benutzererstellung und -änderung neben dem Feld **Alias** eine Schaltfläche hinzugefügt.

  Um einen Alias zu generieren, muss der Clientbenutzer (Operator) auf diese Schaltfläche klicken, die auch die Situation abdeckt, in der der generierte Alias bereits verwendet wird. Durch Klicken auf die Schaltfläche **Generieren** wird die Eindeutigkeitszahl um 1 erhöht und ermöglicht so einen eindeutigen Alias.

- Wenn eine benutzerdefinierte Regel konfiguriert wurde, um Benutzereigenschaften einzuschließen, die normalerweise in den Benutzererstellungsformularen nicht angezeigt werden, wird auf der ActiveRoles Server-Konsole dem Assistenten unter Neues Objekt – Benutzer eine zusätzliche Seite hinzugefügt. Somit können die für die Aliasgenerierung erforderlichen Eigenschaften angegeben werden.
- Die Richtlinie definiert eine Liste von Zeichen, die in E-Mail-Aliasen nicht zulässig sind. Zulässig sind weder Leerzeichen noch die folgenden Zeichen: @ * + | = \ ; : ? [ ] , < > /
- Die Richtlinie führt dazu, dass ActiveRoles Server die Verarbeitung von Vorgangsanforderungen ablehnt, die dem E-Mail-Alias einen leeren Wert zuweisen würden.
- Bei der Überprüfung von Benutzerkonten auf die Richtlinieneinhaltung (siehe weiter unten in diesem Dokument) erkennt und berichtet ActiveRoles Server die Aliase, die nicht so eingerichtet sind, wie die Generierungsrichtlinie für Aliase vorschreibt.

Konfigurieren der Richtlinie „E-Mail-Aliaserzeugung"

Um die Richtlinie „E-Mail-Aliaserzeugung" zu konfigurieren, wählen Sie **E-Mail-Aliaserzeugung** auf der Seite **Zu konfigurierende Richtlinie** im Assistenten für neues Bereitstellungsrichtlinienobjekt oder im Assistenten „Bereitstellungsrichtlinie hinzufügen" aus. Klicken Sie dann auf **Weiter**, um die Seite **Regel zur E-Mail-Aliaserzeugung** anzuzeigen:


Assistent für neues Bereitstellungsrichtlinienobjekt
Regel zur E-Mail-Aliaserzeugung
Richtlinie zur automatischen Einrichtung eines E-Mail-Alias für neu erstellte Benutzerkonten konfigurieren.
E-Mail-Alias setzen auf:
Benutzeranmeldename (Prä-Windows 2000)
Initial des Vornamens gefolgt vom Nachnamen (Beispiel: JSmith)
Vorname gefolgt vom Initial des Nachnamens (Beispiel: JohnS)
Vorname gefolgt vom Nachnamen (Beispiel: JohnSmith)
Andere Kombinationen von Benutzereigenschaften:
Klicken Sie auf "Konfigurieren", um die Regel zur Aliaserzeugung einzurichten.
Konfigurieren...
Manuelle Bearbeitung des E-Mail-Aliasnamens zulassen
Immer
Nur wenn durch diese Richtlinie ein eindeutiger Aliasname generiert werden kann
< Zurück
Weiter >
Abbrechen
Hilfe

Auf der Seite **Regel zur E-Mail-Aliaserzeugung** können Sie eine vorkonfigurierte Regel auswählen oder eine benutzerdefinierte Richtlinie zur E-Mail-Aliasgenerierung erstellen. Die ersten vier Optionen auf der Seite sind selbsterklärend. Beispielsweise erstellt die erste Option einen E-Mail-Alias, der dem Benutzer-Anmeldenamen (Prä-Windows 2000) entspricht. Die Option **Andere Kombinationen von Benutzereigenschaften**, die weiter unten in diesem Abschnitt erörtert wird, ermöglicht das Konfigurieren einer benutzerdefinierten Regel, der auch eine Eindeutigkeitszahl hinzugefügt werden kann.

Durch Aktivieren des Kontrollkästchens **Manuelle Bearbeitung des E-Mail-Aliasnamens zulassen** autorisieren Sie den Operator, der das Benutzerkonto erstellt oder aktualisiert, zum Vornehmen von Änderungen an dem von der Richtlinie generierten Alias. Wenn dieses Kontrollkästchen deaktiviert ist, zeigt ActiveRoles Server in den Formularen zum Erstellen und Ändern von Benutzern das Feld **Alias** schreibgeschützt an.

Indem Sie die Option **Immer** auswählen, autorisieren Sie den Operator, den Alias nach Wunsch zu ändern. Mit der Option **Nur wenn durch diese Richtlinie ein eindeutiger Aliasname generiert werden kann** begrenzen Sie die manuellen Änderungen auf die Situation, in der kein eindeutiger Alias in Übereinstimmung mit den Richtlinienregeln generiert werden kann.

Konfigurieren einer benutzerdefinierten Richtlinie zur E-Mail-Aliasgenerierung

Klicken Sie zum Konfigurieren einer benutzerdefinierten Regel auf **Andere Kombinationen von Benutzereigenschaften**, und klicken Sie dann auf die Schaltfläche **Konfigurieren**. Hierdurch wird das Dialogfeld **Wert konfigurieren** geöffnet, das weiter oben in diesem Kapitel beschrieben wurde (siehe „Konfigurieren einer Richtlinie für die Generierung und Validierung von Eigenschaften"). In diesem Dialogfeld können Sie einen Wert für die Bedingung **„Alias" muss sein** konfigurieren, ähnlich wie beim Konfigurieren der Richtlinie „Erzeugung und Validierung von Eigenschaften".

Um mit dem Konfigurieren eines Wertes zu beginnen, klicken Sie im Dialogfeld **Wert konfigurieren** auf **Hinzufügen**. Nun wird das Fenster **Eintrag hinzufügen** angezeigt.

Ein Wert entsteht durch Verkettung von mindestens einem Eintrag. Im Fenster **Eintrag hinzufügen** können Sie den Typ des hinzuzufügenden Eintrags auswählen und den Eintrag dann konfigurieren. In der folgenden Tabelle werden die verfügbaren Eintragstypen zusammengefasst.

EINTRAGSTYP	BESCHREIBUNG
Text	Fügt dem Wert eine Textzeichenfolge hinzu.
Eindeutigkeitszahl	Fügt einen numerischen Wert hinzu, den die Richtlinie bei einem Aliasnamenskonflikt erhöhen soll.
Benutzereigenschaft	Fügt eine ausgewählte Eigenschaft (oder einen Teil einer Eigenschaft) des Benutzerkontos hinzu, dem die Richtlinie den Alias zuweist.
Eigenschaft der übergeordneten Organisationseinheit	Fügt eine ausgewählte Eigenschaft (oder einen Teil einer Eigenschaft) einer Organisationseinheit in der Containerhierarchie über dem Benutzerkonto hinzu, dem die Richtlinie den Alias zuweist.
Eigenschaft der übergeordneten Domäne	Fügt eine ausgewählte Eigenschaft (oder einen Teil einer Eigenschaft) der Domäne des Benutzerkontos hinzu, dem die Richtlinie den Alias zuweist.

Die Anweisungen zum Konfigurieren eines Eintrags hängen vom Eintragstyp ab. Sie finden Anweisungen für jeden Eintragstyp weiter oben in diesem Kapitel:

- **Text** Siehe Unterabschnitt „Eintragstyp: Text" im Abschnitt „Konfigurieren der Richtlinie „Erzeugung und Validierung von Eigenschaften"".
- **Eindeutigkeitszahl** Siehe Unterabschnitt „Eintragstyp: Eindeutigkeitszahl" im Abschnitt „Konfigurieren der Richtlinie „Erzeugung von Benutzeranmeldenamen"".
- **Benutzereigenschaft** Siehe Unterabschnitt „Eintragstyp: <Objekt> Eigenschaft" im Abschnitt „Konfigurieren der Richtlinie „Erzeugung und Validierung von Eigenschaften"".

- **Eigenschaft der übergeordneten Organisationseinheit** Siehe Unterabschnitt „Eintragstyp: Eigenschaft der übergeordneten Organisationseinheit" im Abschnitt „Konfigurieren der Richtlinie „Erzeugung und Validierung von Eigenschaften"".
- **Eigenschaft der übergeordneten Domäne** Siehe Unterabschnitt „Eintragstyp: Eigenschaft der übergeordneten Domäne" im Abschnitt „Konfigurieren der Richtlinie „Erzeugung und Validierung von Eigenschaften"".

Klicken Sie nach dem Konfigurieren eines Wertes auf **OK**, um das Dialogfeld **Wert konfigurieren** zu schließen. Damit wird der Wert zur Eigenschaftsrichtlinie hinzugefügt. Nötigenfalls können Sie den Wert ändern. Klicken Sie dazu auf die Schaltfläche **Konfigurieren** und verwalten Sie dann die Liste der Einträge im Dialogfeld **Wert konfigurieren**.

Klicken Sie nach dem Konfigurieren der Richtlinienregel auf der Seite **Regel zur E-Mail-Aliaserzeugung** auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schrittweise Anleitungen finden Sie unter **Anleitungen/Verwalten von Richtlinienobjekten/ Konfigurieren von Bereitstellungsrichtlinienobjekten/Konfigurieren einer Richtlinie zur Generierung eines E-Mail-Alias** in der ActiveRoles Server-Hilfe.

Szenario: Generieren von E-Mail-Aliasen anhand von Benutzernamen

Die in diesem Szenario beschriebene Richtlinie generiert den E-Mail-Alias anhand der folgenden Regel: Vorname des Benutzers, optional eine dreistellige Eindeutigkeitszahl, dann ein Punkt und dann der Nachname des Benutzers. Es folgen Beispiele für Aliase, die von dieser Regel generiert werden:

- John.Smith
- John001.Smith
- John002.Smith

Die Richtlinie generiert den Alias John001.Smith für den Benutzer John Smith, falls der Alias John.Smith bereits verwendet wird. Wenn John.Smith und John001.Smith schon verwendet werden, generiert die Richtlinie den Alias John002.Smith, usw.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen und konfigurieren Sie das Richtlinienobjekt, das die entsprechende Richtlinie definiert.
2. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Wenn Sie nun einem Benutzerkonto in dem in Schritt 2 ausgewählten Container einen E-Mail-Alias zuweisen, stellen die Benutzeroberflächen von ActiveRoles Server die Schaltfläche **Generieren** bereit, mit der der Alias in Übereinstimmung mit der Richtlinienregel erstellt werden kann. Wenn Sie im Fall eines Aliasnamenskonflikts auf die Schaltfläche **Generieren** klicken, fügt die Richtlinie dem Alias eine Eindeutigkeitszahl hinzu.

In den folgenden beiden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen und Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt mit dem Assistenten für neues Bereitstellungsrichtlinienobjekt erstellen und konfigurieren. Weitere Informationen über den Assistenten finden Sie unter „Erstellen eines Richtlinienobjekts" im Abschnitt „Verwaltungsaufgaben für Richtlinienobjekte" weiter oben in diesem Kapitel.

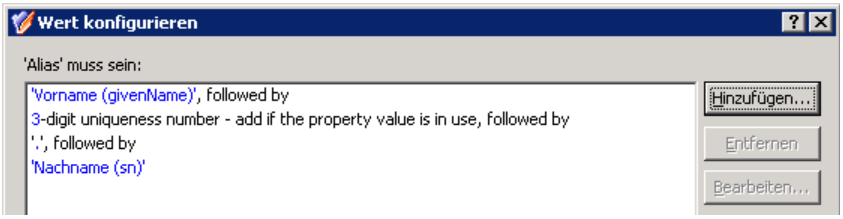
Klicken Sie zum Konfigurieren der Richtlinie auf der Seite **Richtlinientyp auswählen** des Assistenten auf **E-Mail-Aliaserzeugung**. Klicken Sie dann auf **Weiter**.

Klicken Sie auf der Seite **Regel zur E-Mail-Aliaserzeugung** auf **Andere Kombinationen von Benutzereigenschaften** und klicken Sie dann auf **Konfigurieren**.

Füllen Sie das Dialogfeld **Wert konfigurieren** wie folgt aus:

1. Klicken Sie auf **Hinzufügen**.
2. Konfigurieren Sie den Eintrag so, dass er den Vornamen des Benutzers enthält:
   a) Klicken Sie unter **Eintragstyp** auf **Benutzereigenschaft**.
   b) Klicken Sie unter **Eintragseigenschaften** auf **Auswählen**.
   c) Klicken Sie im Fenster **Objekteigenschaft wählen** auf **Vorname** in der Liste **Objekteigenschaft** und klicken Sie dann auf **OK**.
   d) Klicken Sie auf **OK**.
3. Klicken Sie auf **Hinzufügen**.
4. Konfigurieren Sie wie folgt den Eintrag so, dass er optional eine Eindeutigkeitszahl enthält:
   a) Klicken Sie unter **Eintragstyp** auf **Eindeutigkeitszahl**.
   b) Legen Sie unter **Eintragseigenschaften** wie folgt die Eintragsoptionen fest:
      - Klicken Sie auf **Hinzufügen, wenn Eigenschaftswert in Gebrauch ist**.
      - Aktivieren Sie das Kontrollkästchen **Zahl mit fester Länge und voranstehenden Nullen**.
      - Geben Sie in das Feld neben **Länge der Zahl in Stellen** den Wert **3** ein.
   c) Klicken Sie auf **OK**.
5. Klicken Sie auf **Hinzufügen**.
6. Konfigurieren Sie den Eintrag so, dass er einen Punkt enthält:
   a) Geben Sie im Bereich **Textwert** unter **Eintragseigenschaften** einen Punkt ein.
   b) Klicken Sie auf **OK**.
7. Klicken Sie auf **Hinzufügen**.
8. Konfigurieren Sie den Eintrag so, dass er den Nachnamen des Benutzers enthält:
   a) Klicken Sie unter **Eintragstyp** auf **Benutzereigenschaft**.
   b) Klicken Sie unter **Eintragseigenschaften** auf **Auswählen**.
   c) Klicken Sie im Fenster **Objekteigenschaft wählen** auf **Nachname** in der Liste **Objekteigenschaft** und klicken Sie dann auf **OK**.
   d) Klicken Sie auf **OK**.

Nach dem Ausführen dieser Schritte sollte die Liste der Einträge im Dialogfeld **Wert konfigurieren** der folgenden Abbildung ähneln.



Klicken Sie auf **OK**, um das Dialogfeld **Wert konfigurieren** zu schließen. Klicken Sie dann auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schritt 2: Anwenden des Richtlinienobjekts

Sie können das Richtlinienobjekt mit Hilfe der Seite **Richtlinie erzwingen** im Assistenten für neues Bereitstellungsrichtlinienobjekt anwenden oder Sie können den Assistenten erst abschließen und dann den Befehl **Richtlinie erzwingen** für die Domäne, die Organisationseinheit oder die verwaltete Einheit verwenden, auf die Sie die Richtlinie anwenden möchten.

Weitere Informationen über die Anwendung eines Richtlinienobjekts finden Sie unter „Anwenden von Richtlinienobjekten" und „Verwalten des Richtlinienbereichs" weiter oben in diesem Kapitel.

Automatische Bereitstellung von Exchange-Postfächern

Richtlinien dieser Kategorie dienen zum Automatisieren der Auswahl eines Postfachspeichers oder einer Datenbank, wenn ein Benutzer in Microsoft Exchange Server für die Verwendung von Postfächern oder für die Erstellung eines Postfachs aktiviert wird.

Sie können Exchange-Server und Postfachspeicher oder Datenbanken mit zulässiger Postfacherstellung angeben sowie Regeln festlegen, um Postfächer auf mehrere Speicher zu verteilen. Beispielsweise können Sie eine Richtlinie so konfigurieren, dass sie automatisch einen der Speicher mit der geringsten Anzahl von Postfächern auswählt.

Funktionsweise dieser Richtlinie

Wenn ein Benutzer für die Verwendung oder Erstellung von Postfächern aktiviert wird, verwendet ActiveRoles Server diese Richtlinie, um den Postfachspeicher oder die Datenbank auszuwählen. Die Richtlinie definiert einen einzelnen Speicher oder eine Gruppe von Speichern, wo die Erstellung von Postfächern zulässig ist. Es folgen einige spezifische Aspekte des Richtlinienverhaltens:

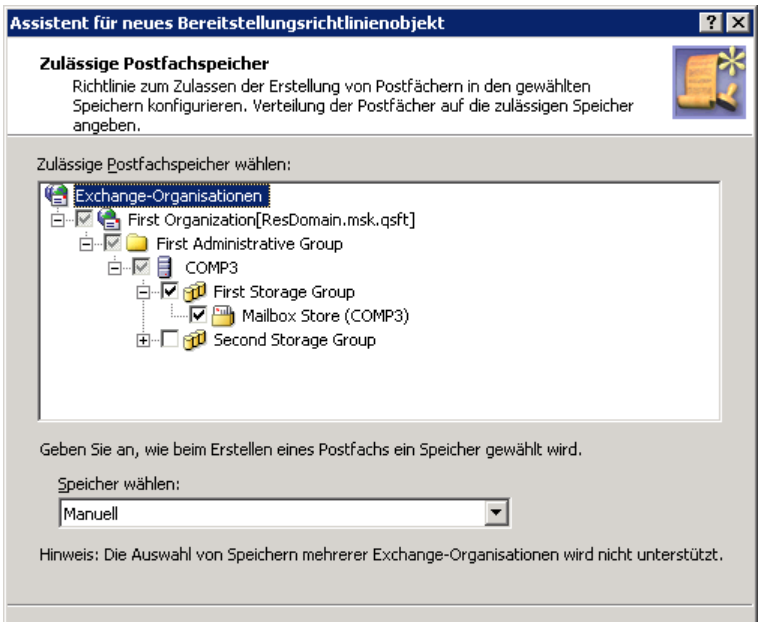
- Wenn die Richtlinie einen einzelnen Speicher angibt, werden Postfächer in diesem Speicher erstellt. Der Operator, der das Benutzerkonto erstellt oder aktualisiert, kann keinen anderen Speicher auswählen.
- Wenn die Richtlinie mehrere Speicher angibt, wird der Speicher automatisch (von ActiveRoles Server) oder manuell (von dem Operator, der das Benutzerkonto erstellt oder aktualisiert) ausgewählt, abhängig von den Richtlinienoptionen.

Im Fall mehrerer Speicher stellt die Richtlinie die folgenden Optionen bereit, um die Speicherauswahl zu steuern:

- **Manuell** Ermöglicht es dem Operator, einen Speicher aus der von der Richtlinie definierten Liste auszuwählen.
- **Durch Anwendung des Kreisverfahrens** Leitet Postfacherstellungs-Anforderungen sequenziell an die Speicher um. Dabei wird der erste Speicher für die erste Anforderung, der zweite Speicher für die zweite Anforderung verwendet usw. Nach dem Erreichen des letzten Speichers wird die nächste Anforderung an den ersten Speicher der Sequenz übergeben.
- **Durch Auswahl des Speichers mit der geringsten Anzahl von Postfächern** Leitet Postfacherstellungs-Anforderungen an den Speicher weiter, der die geringste Anzahl von Postfächern enthält.

Konfigurieren der Richtlinie „Automatische Bereitstellung von Exchange-Postfächern"

Um die Richtlinie „Automatische Bereitstellung von Exchange-Postfächern" zu konfigurieren, wählen Sie **Automatische Bereitstellung von Exchange-Postfächern** auf der Seite **Zu konfigurierende Richtlinie** im Assistenten für neues Bereitstellungsrichtlinienobjekt oder im Assistenten „Bereitstellungsrichtlinie hinzufügen" aus. Klicken Sie dann auf **Weiter**, damit die Seite **Zulässige Postfachspeicher** angezeigt wird.


Assistent für neues Bereitstellungsrichtlinienobjekt
Zulässige Postfachspeicher
Richtlinie zum Zulassen der Erstellung von Postfächern in den gewählten Speichern konfigurieren. Verteilung der Postfächer auf die zulässigen Speicher angeben.
Zulässige Postfachspeicher wählen:
Exchange-Organisationen
First Organization[ResDomain.msk.qsft]
First Administrative Group
COMP3
First Storage Group
Mailbox Store (COMP3)
Second Storage Group
Geben Sie an, wie beim Erstellen eines Postfachs ein Speicher gewählt wird.
Speicher wählen:
Manuell
Hinweis: Die Auswahl von Speichern mehrerer Exchange-Organisationen wird nicht unterstützt.

Auf dieser Seite können Sie die Server und Postfachspeicher oder Datenbanken auswählen, die für die Postfacherstellung zulässig sein sollen. Wählen Sie Postfachspeicher aus einer einzelnen Exchange-Organisation aus. Das Auswählen von Postfachspeichern oder Datenbanken aus mehreren Organisationen wird nicht unterstützt.

Wenn Sie mehrere Speicher auswählen, können Sie angeben, wie bei einer Postfacherstellungsanforderung ein Speicher ausgewählt werden soll. Wählen Sie in der Liste **Speicher wählen** eine der folgenden Optionen aus, die weiter oben in diesem Abschnitt erörtert werden:

- Manuell
- Durch Anwendung des Kreisverfahrens
- Anhand der geringsten Anzahl von Postfächern

Klicken Sie nach Abschluss des Vorgangs auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schrittweise Anleitungen finden Sie unter **Anleitungen/Verwalten von Richtlinienobjekten/ Konfigurieren von Bereitstellungsrichtlinienobjekten/Konfigurieren einer Richtlinie zur automatischen Bereitstellung von Exchange-Postfächern** in der ActiveRoles Server-Hilfe.

Szenario: Lastenausgleich für Postfachspeicher

Mit der in diesem Szenario beschriebenen Richtlinie können mehrere Speicher für die Postfacherstellung verwendet werden, und ActiveRoles Server wählt automatisch den Speicher mit der kleinsten Anzahl von Postfächern aus.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen und konfigurieren Sie ein Richtlinienobjekt, das die entsprechende Richtlinie definiert.
2. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Wenn Sie ein Postfach für ein Benutzerkonto erstellen, das sich in dem in Schritt 2 ausgewählten Container befindet, wählt ActiveRoles Server daher aus den Speichern, in denen die Postfacherstellung zulässig ist, den am wenigsten ausgelasteten.

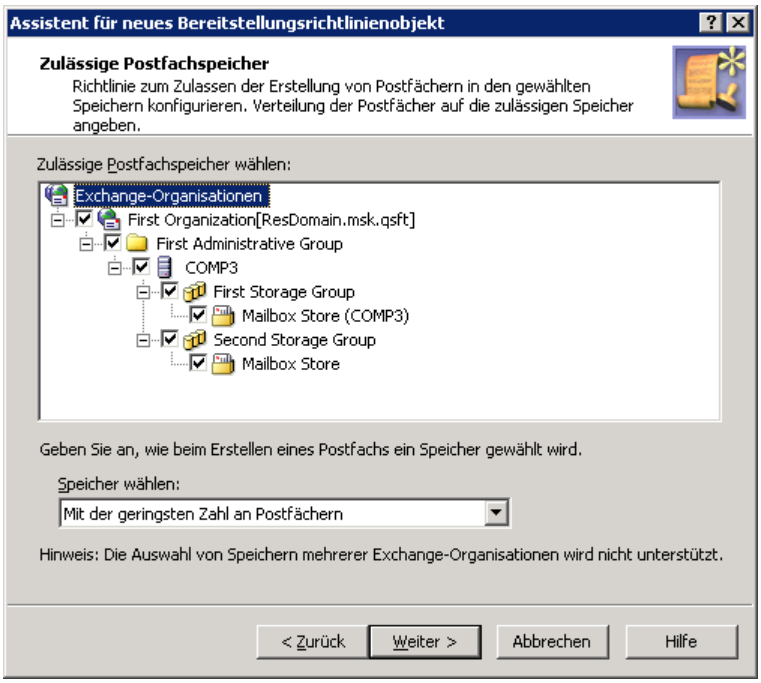
In den folgenden beiden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen und Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt mit dem Assistenten für neues Bereitstellungsrichtlinienobjekt erstellen und konfigurieren. Weitere Informationen über den Assistenten finden Sie unter „Erstellen eines Richtlinienobjekts“ im Abschnitt „Verwaltungsaufgaben für Richtlinienobjekte“ weiter oben in diesem Kapitel.

Klicken Sie zum Konfigurieren der Richtlinie auf der Seite **Richtlinientyp auswählen** des Assistenten auf **Automatische Bereitstellung von Exchange-Postfächern**. Klicken Sie dann auf **Weiter**.

Wählen Sie auf der Seite **Zulässige Postfachspeicher** die Speicher, in denen die Postfacherstellung zulässig sein soll. Klicken Sie dann unter **Speicher wählen** auf **Mit der geringsten Zahl an Postfächern**, wie in der folgenden Abbildung gezeigt.


Assistent für neues Bereitstellungsrichtlinienobjekt
Zulässige Postfachspeicher
Richtlinie zum Zulassen der Erstellung von Postfächern in den gewählten Speichern konfigurieren. Verteilung der Postfächer auf die zulässigen Speicher angeben.
Zulässige Postfachspeicher wählen:
Exchange-Organisationen
First Organization[ResDomain.msk.qsft]
First Administrative Group
COMP3
First Storage Group
Mailbox Store (COMP3)
Second Storage Group
Mailbox Store
Geben Sie an, wie beim Erstellen eines Postfachs ein Speicher gewählt wird.
Speicher wählen:
Mit der geringsten Zahl an Postfächern
Hinweis: Die Auswahl von Speichern mehrerer Exchange-Organisationen wird nicht unterstützt.
< Zurück
Weiter >
Abbrechen
Hilfe

Klicken Sie auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schritt 2: Anwenden des Richtlinienobjekts

Sie können das Richtlinienobjekt mit Hilfe der Seite **Richtlinie erzwingen** im Assistenten für neues Bereitstellungsrichtlinienobjekt anwenden oder Sie können den Assistenten erst abschließen und dann den Befehl **Richtlinie erzwingen** für die Domäne, die Organisationseinheit oder die verwaltete Einheit verwenden, auf die Sie die Richtlinie anwenden möchten.

Weitere Informationen über die Anwendung eines Richtlinienobjekts finden Sie unter „Anwenden von Richtlinienobjekten“ und „Verwalten des Richtlinienbereichs“ weiter oben in diesem Kapitel.

Standardmäßige Erstellungsoptionen für ein Exchange-Postfach

Im Assistenten für die Erstellung von Benutzerkonten – ganz gleich, ob in der ActiveRoles Server-Konsole oder im Web-Interface – ist die Option **Exchange-Postfach erstellen** standardmäßig ausgewählt, wodurch das Benutzerpostfach bei Erstellung eines Benutzerkontos erstellt wird. Dieses Verhalten kann durch Anwenden einer entsprechend entworfenen Richtlinie auf die Kategorie „Automatische Bereitstellung des Exchange-Postfachs“ geändert werden.

Eine Richtlinie kann so konfiguriert werden, dass die Option **Exchange-Postfach erstellen** nicht standardmäßig ausgewählt ist, sondern der Administrator, der den Assistenten für die Erstellung eines Benutzerkontos verwendet, diese Option bei Bedarf auswählen kann. Es ist außerdem möglich, eine Richtlinie zu konfigurieren, die die Auswahl der Option **Exchange-Postfach erstellen** forciert.

Gehen Sie folgendermaßen vor, um standardmäßige Erstellungsoptionen für ein Exchange-Postfach festzulegen:

1. Erstellen Sie ein Richtlinienobjekt, das eine Richtlinie zur automatischen Bereitstellung von Exchange-Postfächern enthält.
2. Öffnen Sie das Dialogfeld **Eigenschaften** für das von Ihnen erstellte Richtlinienobjekt.
3. Doppelklicken Sie auf der Registerkarte **Richtlinien** im Dialogfeld **Eigenschaften** auf den Richtlinieneintrag „Automatische Bereitstellung von Exchange-Postfächern".
4. Legen Sie auf der Registerkarte **Postfacherstellung** im Dialogfeld **Eigenschaften der Richtlinie zur automatischen Bereitstellung von Exchange-Postfächern** Ihrer Situation entsprechende Richtlinienoptionen fest:
   - **Benutzerpostfach standardmäßig erstellen** Legt fest, ob die Option **Exchange-Postfach erstellen** standardmäßig im Assistenten zur Erstellung von Benutzerkonten aktiviert ist oder nicht. Wenn der Benutzer Postfächer nicht standardmäßig erstellen soll, deaktivieren Sie diese Richtlinienoption.
   - **Erstellung des Postfachs erzwingen** Führt dazu, dass die Option **Exchange-Postfach erstellen** aktiviert und nicht verfügbar ist, sodass der Administrator, der ein Benutzerkonto erstellt, diese Option nicht deaktivieren kann.
5. Klicken Sie auf **OK**, um die von Ihnen geöffneten Dialogfelder zu schließen.
6. Wenden Sie das Richtlinienobjekt auf den Bereich an (Domänen, Container oder verwaltete Einheiten), in dem diese Richtlinie gelten soll.

Automatische Bereitstellung des Stammordners

Richtlinien dieser Kategorie automatisieren die Erstellung oder Umbenennung von Benutzerstammordnern und -stammfreigaben bei der Erstellung oder Umbenennung von Benutzerkonten mit ActiveRoles Server.

Sie können einen Server angeben, auf dem Stammordner und Stammfreigaben erstellt werden sollen. Sie können definieren, wie Berechtigungen für neue Stammordner und -freigaben festgelegt werden. Sie können Namenskonventionen für neue Stammordner und Stammfreigaben angeben, und Sie können die Anzahl gleichzeitiger Verbindungen mit Stammfreigaben beschränken.

Beispielsweise kann mit Richtlinien dieses Typs eine Unternehmensregel definiert werden, mit der bei jeder Benutzerkontoerstellung in ActiveRoles Server auch ein Ordner in einer Netzwerkdateifreigabe erstellt und als Stammordner des Benutzers zugewiesen wird.

Funktionsweise dieser Richtlinie

Bei der Ausführung der Richtlinie „Automatische Bereitstellung des Stammordners" führt ActiveRoles Server diverse Aktionen aus, je nachdem, ob ein Benutzer erstellt, kopiert oder umbenannt wird.

Erstellen von Stammordnern und -freigaben bei der Erstellung von Benutzerkonten

Wenn ActiveRoles Server ein Benutzerkonto erstellt (unabhängig davon, ob von Grund auf neu oder durch Kopieren eines vorhandenen Kontos), kann die Richtlinie dazu führen, dass ActiveRoles Server einen Stammordner und optional eine Stammfreigabe für das Konto, das den in der Richtlinie angegebenen Pfad nutzt, erstellt. Der Name der Stammfreigabe setzt sich aus dem Benutzernamen und dem in der Richtlinie angegebenen Präfix und Suffix zusammen.

Die Richtlinie bietet die Möglichkeit, die Erstellung von Stammordnern mit Pfaden und Namen, die sich von dem durch die Richtlinie vorgegebenen Pfad und Namen unterscheiden, zu aktivieren. Beispielsweise kann die Richtlinie „Erzeugung und Validierung von Eigenschaften" so konfiguriert werden, dass sie die Eigenschaften **Stammlaufwerk** und **Stammverzeichnis** für Benutzerkonten generiert. Wenn Sie Änderungen an diesen Eigenschaften vornehmen, prüft ActiveRoles Server, ob der angegebene Stammordner vorhanden ist, und erstellt gegebenenfalls den Stammordner.

In ActiveRoles Server ist eine spezielle Richtlinie implementiert, die die Ordner in Netzwerkdateifreigaben beschränkt, in denen Stammordner erstellt werden können. Das Richtlinienobjekt, das diese Richtlinie enthält, befindet sich im Container **Configuration/Policies/Administration/Builtin**. Der Name des Richtlinienobjekts lautet **Built-in Policy – Home Folder Location Restriction**. Sie können es mit Hilfe der ActiveRoles Server-Konsole aufrufen. Die Richtlinieneinstellungen umfassen eine Liste der Ordner in den Netzwerkdateifreigaben, in denen die Erstellung von Stammordnern zulässig ist. Anweisungen bezüglich der Anzeige oder Änderung dieser Liste finden Sie unter „Konfigurieren der Richtlinie 'Einschränkungen bezüglich des Speicherorts von Stammordnern'" weiter unten in diesem Abschnitt.

Umbenennen von Stammordnern beim Umbenennen von Benutzerkonten

Wenn ActiveRoles Server den Benutzer-Anmeldenamen (Prä-Windows 2000) eines Benutzerkontos ändert, kann die Richtlinie den Stammordner umbenennen und optional die Stammfreigabe für dieses Benutzerkonto neu erstellen. Der Name der neuen Stammfreigabe wird gemäß den in der Richtlinie angegebenen Namenskonventionen erstellt.

Die Richtlinie benennt den vorhandenen Stammordner anhand des neuen Benutzer-Anmeldenamens (Prä-Windows 2000) um. Wenn der Stammordner allerdings gerade verwendet wird, kann ActiveRoles Server ihn nicht umbenennen. In diesem Fall erstellt ActiveRoles Server einen neuen Stammordner mit dem neuen Namen und verändert den vorhandenen Stammordner nicht.

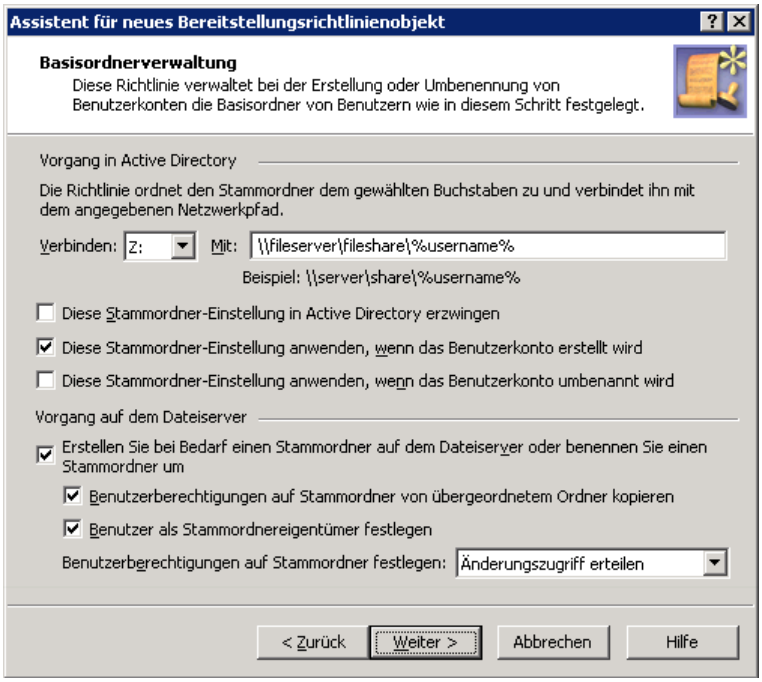
Option zur Vermeidung eines Vorgangs auf dem Dateiserver

Standardmäßig versucht ActiveRoles Server, einen (nicht lokalen) Stammordner auf dem Dateiserver zu erstellen oder umzubenennen, wenn die Eigenschaft „Stammverzeichnis" für ein Benutzerkonto in Active Directory gesetzt oder geändert wird. Wenn die Erstellung oder Umbenennung des Stammordners fehlschlägt (zum Beispiel weil der Zugriff auf den Dateiserver nicht möglich ist), dann schlägt die Erstellung oder Änderung des Benutzerkontos ebenfalls fehl. Um eine solche Fehlerbedingung zu vermeiden, kann eine Richtlinie für die automatische Bereitstellung von Stammordnern so konfiguriert werden, dass ActiveRoles Server die Änderungen auf die Eigenschaften **Stammlaufwerk** und **Stammverzeichnis** in Active Directory anwendet, ohne einen Vorgang auf dem Dateiserver zu versuchen. Diese Richtlinienoption ermöglicht die Verwendung eines anderen Tools als ActiveRoles Server für die Erstellung von Stammordnern auf dem Dateiserver.

ActiveRoles Server umfasst ein vorkonfiguriertes Richtlinienobjekt, das die Erstellung oder Umbenennung von Stammordnern bei der Festlegung von Stammordnereigenschaften für Benutzerkonten in Active Directory ermöglicht. Das Richtlinienobjekt befindet sich im Container **Configuration/Policies/Administration/Builtin** in der ActiveRoles Server-Konsolenstruktur. Der Name des Richtlinienobjekts lautet **Built-in Policy – Default Rules to Provision Home Folders**. Wenn Sie verhindern möchten, dass ActiveRoles Server versucht, Stammordner zu erstellen oder umzubenennen, können Sie die Richtlinie im integrierten Richtlinienobjekt ändern oder eine andere Richtlinie für die automatische Bereitstellung von Stammordnern erstellen und konfigurieren, bei der die entsprechende Option deaktiviert ist.

Konfigurieren der Richtlinie „Automatische Bereitstellung des Stammordners"

Um die Richtlinie „Automatische Bereitstellung des Stammordners" zu konfigurieren, wählen Sie **Automatische Bereitstellung des Stammordners** auf der Seite **Zu konfigurierende Richtlinie** im Assistenten für neues Bereitstellungsrichtlinienobjekt oder im Assistenten „Bereitstellungsrichtlinie hinzufügen" aus. Klicken Sie dann auf **Weiter**, damit die Seite **Basisordnerverwaltung** angezeigt wird.


Assistent für neues Bereitstellungsrichtlinienobjekt
Basisordnerverwaltung
Diese Richtlinie verwaltet bei der Erstellung oder Umbenennung von Benutzerkonten die Basisordner von Benutzern wie in diesem Schritt festgelegt.
Vorgang in Active Directory
Die Richtlinie ordnet den Stammordner dem gewählten Buchstaben zu und verbindet ihn mit dem angegebenen Netzwerkpfad.
Verbinden: Z:
Mit: \\fileserver\fileshare\%username%
Beispiel: \\server\share\%username%
Diese Stammordner-Einstellung in Active Directory erzwingen
Diese Stammordner-Einstellung anwenden, wenn das Benutzerkonto erstellt wird
Diese Stammordner-Einstellung anwenden, wenn das Benutzerkonto umbenannt wird
Vorgang auf dem Dateiserver
Erstellen Sie bei Bedarf einen Stammordner auf dem Dateiserver oder benennen Sie einen Stammordner um
Benutzerberechtigungen auf Stammordner von übergeordnetem Ordner kopieren
Benutzer als Stammordnereigentümer festlegen
Benutzerberechtigungen auf Stammordner festlegen: Änderungszugriff erteilen
< Zurück
Weiter >
Abbrechen
Hilfe

Auf dieser Seite können Sie die folgenden Optionen konfigurieren.

Verbinden Sie *<Laufwerksbuchstabe>* mit *<Netzwerkpfad>*

Bei der Erstellung oder Umbenennung eines Benutzerkontos kann die Richtlinie das Benutzerkonto in Active Directory so konfigurieren, dass sie den Stammordner mit dem angegebenen Netzwerkpfad verbindet. Wählen Sie in der Liste **Verbinden** den Laufwerksbuchstabe des Laufwerks aus, dem die Richtlinie den Stammordner zuordnen soll. Geben Sie im Feld **Mit** einen Netzwerkpfad zum Stammordner ein. Vergewissern Sie sich, dass der Pfad den folgenden Anforderungen entspricht:

- Ein gültiger Netzwerkpfad muss mit dem UNC-Namen einer Netzwerkdateifreigabe wie etwa \\Server\Freigabe\ beginnen und normalerweise die Angabe %Benutzername% umfassen. Bei Auswahl der Richtlinieneinstellung **Verbinden: Z: Mit: \\Server\Share\%username%**, die Richtlinie kann ein Benutzerkonto in Active Directory so konfigurieren, dass die Eigenschaft **Stammlaufwerk** des Benutzerkontos auf Z: und die Eigenschaft **Stammverzeichnis** des Benutzerkontos auf \\Server\Freigabe\Anmeldename gesetzt ist, wobei „Anmeldename" für den Prä-Windows 2000-Anmeldenamen des Benutzerkontos steht.
- Der Pfad muss eine gemeinsame Freigabe enthalten, die sich auf der Ebene direkt über den Stammordnern befindet. Wenn Sie beispielsweise **\\Comp\Home\%Benutzername%** eingeben, erstellt die Richtlinie Stammordner in der Netzwerkfreigabe **home** auf dem Server **comp**, wobei der Name des Ordners identisch mit dem Benutzeranmeldenamen (Prä-Windows 2000) ist. Der Pfad **\\comp\%Benutzername%** ist ungültig.

- Der Ordner in der Netzwerkdateifreigabe, in der die Richtlinie Stammordner erstellen soll, muss in der Richtlinie „Einschränkungen bezüglich des Speicherorts von Stammordnern" aufgelistet sein. Anweisungen bezüglich der Anzeige oder Änderung der Liste finden Sie unter „Konfigurieren der Richtlinie 'Einschränkungen bezüglich des Speicherorts von Stammordnern'" weiter unten in diesem Abschnitt.
- Wenn Sie möchten, dass die Richtlinie Stammfreigaben erstellt (siehe Informationen über die Seite **Stammfreigabenverwaltung** weiter unten in diesem Abschnitt), dann dürfen Sie *keine* administrative Freigabe wie etwa C$ als die allgemeine Freigabe im Feld **Mit** angeben. Andernfalls kann die Richtlinie bei der Erstellung von Stammordnern möglicherweise keine Stammfreigaben erstellen. Wenn Sie also **\\comp\C$\%Benutzername%** angeben, kann die Richtlinie erfolgreich Stammordner im Ordner **C:** auf dem Computer **Comp** erstellen, jedoch keine Stammfreigaben erstellen.

Diese Stammordner-Einstellung in Active Directory erzwingen

Verwenden Sie diese Option, damit ActiveRoles Server überprüft, ob de Eigenschaften **Stammlaufwerk** und **Stammverzeichnis** für Benutzerkonten in Active Directory mit der von dieser Richtlinie angegebenen Einstellung **Verbinden: <*Laufwerksbuchstabe*> Mit:<*Netzwerkpfad*>** konform ist.

So führt diese Option zum Beispiel mit der Richtlinieneinstellung **Verbinden: Z: Mit: \\Server\Freigabe\%Benutzername%** bei dem Versuch, ein Benutzerkonto dahingehend zu ändern, dass der Eigenschaft **Stammlaufwerk** ein anderer Laufwerksbuchstabe als Z: zugewiesen wird, zu einem Richtlinienverstoß in ActiveRoles Server. Gleiches gilt, wenn der Eigenschaft **Stammverzeichnis** ein anderer Netzwerkpfad als \\Server\Freigabe\Anmeldename zugewiesen wird, wobei „Anmeldename" für den Prä-Windows 2000-Anmeldenamen des Benutzerkontos steht.

Wenn diese Option deaktiviert ist, ermöglicht die Richtlinie, dass sich Stammordnerpfad und -name von dem durch die Richtlinie vorgegebenen Pfad und Namen unterscheiden. Es kann eine Richtlinie zur Erzeugung und Validierung von Eigenschaften konfiguriert werden, die die Eigenschaften **Stammlaufwerk** und **Stammverzeichnis** für Benutzerkonten erstellt. Diese Eigenschaften können auch manuell angegeben werden. In beiden Fällen aktualisiert ActiveRoles Server das Benutzerkonto, sodass der Ordner mit dem angegebenen Pfad und Namen als Stammordner des Benutzers festgelegt wird. Erforderlichenfalls erstellt ActiveRoles Server den Ordner.

Wenn diese Option aktiviert ist, verhält sich die Richtlinie wie folgt:

- Sie gewährleistet, dass der Pfad und der Name des Stammordners den Richtlinien-einstellungen entsprechen. Wenn bei der Erstellung oder Änderung eines Benutzerkontos ein anderer Pfad oder Name angegeben wird, ermöglicht die Richtlinie nicht das Senden des Stammordnerpfads und -namens an das Verzeichnis.
- Der Befehl **Richtlinie prüfen** führt dazu, dass die Richtlinie die bestehenden Stammordner-einstellungen überprüft. Die Richtlinie überprüft die Ergebnisse über Richtlinienverstöße (falls vorhanden) und bietet die Möglichkeit, die Stammordnerpfad- und -namenseinstellungen von Benutzerkonten zu korrigieren, damit diese den Richtlinieneinstellungen entsprechen.

Aktivieren Sie das Kontrollkästchen **Diese Stammverzeichniseinstellung in Active Directory erzwingen**, um zu gewährleisten, dass die Stammordner für Benutzerkonten entsprechend dieser Richtlinie eingerichtet werden.

Wenn Sie das Kontrollkästchen deaktivieren, haben Sie die Möglichkeit, die Richtlinie „Erzeugung und Validierung von Eigenschaften" anzuwenden, um die Eigenschaften „Stammlaufwerk" und „Stammverzeichnis" zu generieren und zu validieren. In diesem Fall erstellt ActiveRoles Server Stammordner in Übereinstimmung mit den flexiblen, in hohem Maß anpassbaren Richtlinienregeln, die von der Richtlinie „Erzeugung und Validierung von Eigenschaften" bereitgestellt werden, und ordnet diese dem Stammordner zu.

Wenn Sie die Eigenschaften **Stammlaufwerk** und **Stammverzeichnis** festlegen, erstellt ActiveRoles Server den Stammordner nicht, wenn der Netzwerkpfad zu dem Ordner, in dem sich der Stammordner befinden soll, nicht in der Richtlinie Einschränkung bezüglich des Speicherorts des Stammordners aufgelistet ist. Die Richtlinie definiert eine Liste zu den Ordnern in Netzwerkdateifreigaben, in denen die Erstellung von Stammordnern zulässig ist, und verhindert, dass ActiveRoles Server Stammordner an anderen Netzwerkspeicherplätzen erstellt. Anweisungen bezüglich der Anzeige oder Änderung dieser Richtlinieneinstellungen finden Sie unter „Konfigurieren der Richtlinie 'Einschränkungen bezüglich des Speicherorts von Stammordnern'" weiter unten in diesem Abschnitt.

Diese Stammordner-Einstellung anwenden, wenn das Benutzerkonto erstellt wird

Bei Erstellung eines Benutzerkontos führt diese Option dazu, dass ActiveRoles Server das Benutzerkonto in Active Directory so konfiguriert, dass es mit der durch diese Richtlinie festgelegten Einstellung **Verbinden: *<Laufwerksbuchstabe>* Mit:*<Netzwerkpfad>*** konform ist.

So führt diese Option zum Beispiel mit der Richtlinieneinstellung **Verbinden: Z: Mit: \\Server\Freigabe\%Benutzername%** dazu, dass die Aktivierung dieses Kontrollkästchens gewährleistet, dass die Eigenschaft **Stammverzeichnis** für ein neu erstelltes Benutzerkonto auf Z: und die Eigenschaft **Stammverzeichnis** auf \\Server\Freigabe\Anmeldename gesetzt ist, wobei Anmeldename für den Prä-Windows 2000-Anmeldenamen des Benutzerkontos steht.

Diese Stammordner-Einstellung anwenden, wenn das Benutzerkonto umbenannt wird

Beim Umbenennen eines Benutzerkontos führt diese Option dazu, dass ActiveRoles Server das Benutzerkonto in Active Directory so konfiguriert, dass es mit der durch diese Richtlinie festgelegten Einstellung **Verbinden: *<Laufwerksbuchstabe>* Mit: *<Netzwerkpfad>*** konform ist.

Bei Auswahl der Richtlinieneinstellung **Verbinden: Z: Mit: \\Server\Freigabe\%Benutzername%** beispielsweise führt die Umbenennung eines Benutzerkontos dazu, dass die Richtlinie die Eigenschaft **Stammverzeichnis** auf \\Server\Freigabe\NeuerAnmeldename setzt, wobei „NeuerAnmeldename" für den Prä-Windows 2000-Anmeldenamen steht, der dem Benutzerkonto durch den Umbenennungs-vorgang zugewiesen wird.

Erstellen Sie bei Bedarf einen Stammordner auf dem Dateiserver oder benennen Sie einen Stammordner um

st diese Option ausgewählt, so weist Sie ActiveRoles Server an, die Erstellung oder Umbenennung eines (nicht lokalen) Stammordners auf dem Dateiserver zu versuchen, wenn die Eigenschaft **Stammverzeichnis** für ein Benutzerkonto in Active Directory gesetzt oder geändert wird. Die Umbenennung des Stammordners wird versucht, wenn der Eigenschaftswert **Stammverzeichnis** die Angabe %Benutzername% enthält und die Änderungen am Benutzerkonto die Änderung des Prä-Windows 2000-Anmeldenamens des Benutzerkontos umfasst. In allen anderen Fällen wird versucht, einen neuen Stammordner zu erstellen.

So versucht ActiveRoles Server beispielsweise bei der Richtlinieneinstellung **Verbinden: Z: Mit: \\Server\Freigabe\%Benutzername%** und Aktivierung dieses Kontrollkästchens zusammen mit der Option zur Anwendung der Richtlinieneinstellung bei Erstellung eines Benutzerkontos, den Stammordner für das Benutzerkonto zu erstellen. ActiveRoles Server versucht, den Ordner mit dem folgenden Netzwerkpfad zu erstellen: \\Server\Freigabe\Anmeldename, wobei „Anmeldename" für den Prä-Windows 2000-Anmeldenamen des Benutzerkontos steht.

Ein weiteres Beispiel ist die Konfiguration der Eigenschaften **Stammlaufwerk** und **Stammverzeichnis** für ein vorhandenes Benutzerkonto in Active Directory: Bei Aktivierung dieses Kontrollkästchens versucht ActiveRoles Server, den Ordner zu erstellen, der durch den Netzwerkpfad angegeben ist, der der Eigenschaft **Stammverzeichnis** zugewiesen ist.

Wenn die Erstellung oder Umbenennung des Stammordners auf dem Dateiserver fehlschlägt, dann schlägt die Erstellung oder Änderung des Benutzerkontos ebenfalls fehl. Um eine solche Fehlerbedingung zu vermeiden, können Sie dieses Kontrollkästchen deaktivieren. Dies führt dazu, dass ActiveRoles Server die Änderungen auf die Eigenschaften Eigenschaften **Stammlaufwerk** und **Stammverzeichnis** in Active Directory anwendet, ohne einen Vorgang auf dem Dateiserver zu unternehmen, was die Verwendung eines anderen Tools für die Erstellung von Stammordnern auf dem Dateiserver ermöglicht.

Benutzerberechtigungen auf Stammordner von übergeordnetem Ordner kopieren

Bei der Erstellung oder Umbenennung eines Stammordners für ein bestimmtes Benutzerkonto gewährleistet diese Option, dass das Benutzerkonto über dieselben Rechte in Bezug auf den Stammordner verfügt, die es auch in Bezug auf den Ordner hat, in dem sich der Stammordner befindet.

Benutzer als Stammordnereigentümer festlegen

Bei der Erstellung oder Umbenennung eines Stammordners für ein bestimmtes Benutzerkonto gewährleistet diese Option, dass das Benutzerkonto als Besitzer des Stammordners festgelegt wird.

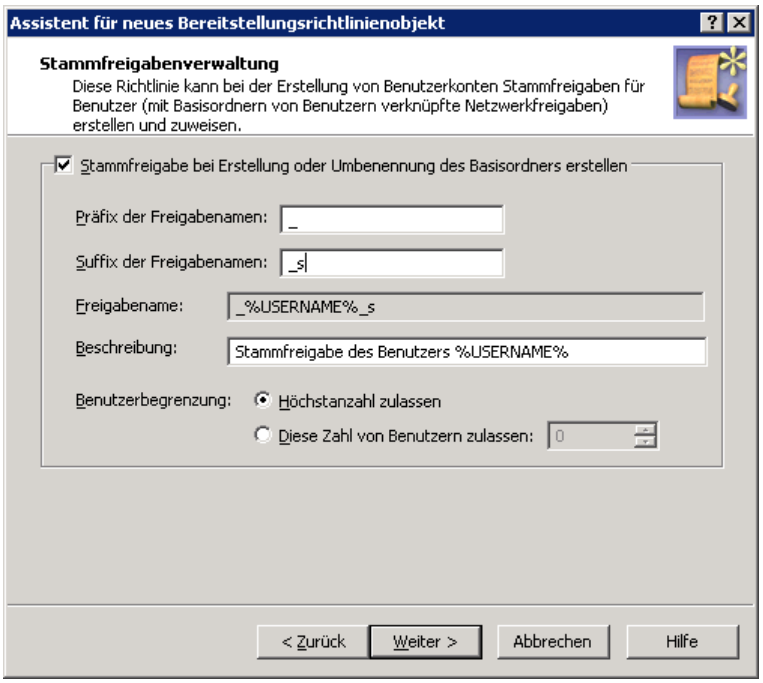
Ein Besitzer eines Ordners ist autorisiert, beliebige Änderungen an den Berechtigungseinstellungen für den Ordner durchzuführen. Ein Besitzer kann zum Beispiel anderen Personen den Zugriff auf den Ordner gewähren.

Benutzerberechtigungen für Stammordner festlegen

Bei der Erstellung oder Umbenennung eines Stammordners für ein bestimmtes Benutzerkonto gewährleistet diese Option, dass das Benutzerkonto über die spezifischen Zugriffsrechte für den Stammordner verfügt.

Mit der Einstellung **Vollzugriff gewähren** ist das Benutzerkonto autorisiert, jegliche Vorgänge am Ordner und seinen Inhalten durchzuführen. Ausnahme: Änderungen an den Berechtigungseinstellungen. Bei Aktivierung der Option **Vollzugriff gewähren** ist das Benutzerkonto autorisiert, den Inhalt des Ordners anzuzeigen und zu ändern.

Klicken Sie danach auf **Weiter**, um die Seite **Stammfreigabenverwaltung** anzuzeigen. Auf dieser Seite können Sie Richtlinienoptionen für die Erstellung von Stammfreigaben konfigurieren:


Assistent für neues Bereitstellungsrichtlinienobjekt
Stammfreigabenverwaltung
Diese Richtlinie kann bei der Erstellung von Benutzerkonten Stammfreigaben für Benutzer (mit Basisordnern von Benutzern verknüpfte Netzwerkfreigaben) erstellen und zuweisen.
Stammfreigabe bei Erstellung oder Umbenennung des Basisordners erstellen
Präfix der Freigabenamen: _
Suffix der Freigabenamen: _s
Freigabename: _%USERNAME%_s
Beschreibung: Stammfreigabe des Benutzers %USERNAME%
Benutzerbegrenzung: Höchstanzahl zulassen
Diese Zahl von Benutzern zulassen: 0
< Zurück
Weiter >
Abbrechen
Hilfe

Damit die Richtlinie Stammfreigaben erstellt, aktivieren Sie das Kontrollkästchen **Stammfreigabe bei Erstellung oder Umbenennung des Basisordners erstellen**.

Wenn Sie die Richtlinie für die Erstellung von Stammfreigaben konfigurieren, können Sie das Präfix und Suffix für die Stammfreigabenamen angeben.

Indem Sie ein Präfix und Suffix angeben, können Sie eine Namenskonvention für Stammfreigaben einrichten. Nehmen Sie beispielsweise an, dass Sie Stammfreigaben ganz oben in der Freigabenliste anzeigen möchten. Verwenden Sie dazu als Präfix einen Unterstrich. Sie können auch ein Suffix zuweisen, um von der Richtlinie erstellte Stammfreigaben besonders zu kennzeichnen. Um beispielsweise die Stammfreigaben von Benutzern aus der Sales-Abteilung zu kennzeichnen, können Sie das Suffix _s verwenden. Wenn Sie nun ein Benutzerkonto mit dem Benutzer-Anmeldenamen JohnB (Prä-Windows 2000) erstellen, ordnet die Richtlinie den Stammordner des Benutzers dem ausgewählten Laufwerk zu und gibt **\\Server_JohnB_s** als Pfad zum Stammordner an. Die Richtlinie erstellt außerdem die Freigabe _**JohnB_s**, die auf den Ordner **\\Server\Home\JohnB** zeigt.

Optional können sie in das Feld **Beschreibung** einen Kommentar zu der Stammfreigabe eingeben. Dieser ist für die Benutzer sichtbar, wenn sie Freigabeeigenschaften anzeigen.

Sie können auch die Anzahl der Benutzer begrenzen, die gleichzeitig eine Verbindung mit der Freigabe herstellen können. Klicken Sie dazu auf **Höchstanzahl zulassen** oder **Diese Zahl von Benutzern zulassen**. Geben Sie bei der letzteren Option in das Feld neben der Option eine Zahl ein.

Schrittweise Anleitungen finden Sie unter **Anleitungen/Verwalten von Richtlinienobjekten/Konfigurieren von Bereitstellungsrichtlinienobjekten/Konfigurieren einer Richtlinie zur automatischen Bereitstellung eines Stammverzeichnisses** in der ActiveRoles Server-Hilfe.

Verwenden der integrierten Richtlinie für die Bereitstellung des Stammordners

Wenn Sie ActiveRoles Server so konfigurieren möchten, dass die Festlegung oder Änderung von mit dem Stammordner in Verbindung stehenden Eigenschaften für ein beliebiges Benutzerkonto in einer beliebigen verwalteten Domäne nicht zu dem Versuch der Erstellung oder Umbenennung eines Ordners auf einem Dateiserver führt, dann können Sie die ActiveRoles Server-Konsole verwenden, um das integrierte Richtlinienobjekt zu ändern:

1. Wählen Sie in der Konsolenstruktur **Configuration | Policies | Administration | Builtin**.
2. Doppelklicken Sie im Bereich „Details" auf **Built-in Policy – Default Rules to Provision Home Folders**.
3. Wählen Sie auf der Registerkarte **Richtlinien** die Richtlinie aus der Liste aus und klicken Sie dann auf **Anzeigen/Bearbeiten**.
4. Deaktivieren Sie auf der Registerkarte **Stammverzeichnis** das Kontrollkästchen **Stammverzeichnis auf Dateiserver bei Bedarf erstellen oder umbenennen**.
5. Klicken Sie auf **OK**, um die von Ihnen geöffneten Dialogfelder zu schließen.

Wenn Sie über andere Richtlinienobjekte verfügen, die Richtlinien der Kategorie „Automatische Stammordner-Bereitstellung" enthalten, dann müssen Sie sie entsprechend konfigurieren: Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Stammverzeichnis auf Dateiserver bei Bedarf erstellen oder umbenennen** in jeder dieser Richtlinien abhängig davon, ob ActiveRoles Server die Erstellung oder Umbenennung von Stammordnern für Benutzerkonten versuchen soll, die in den Bereich des entsprechenden Richtlinienobjekts fallen.

In einer anderen Situation kann es erforderlich sein, dass ActiveRoles Server Stammordner für Benutzerkonten erstellen oder umbenennen soll, die sich außerhalb eines bestimmten Bereichs befinden (wie etwa eine bestimmte Domäne, Organisationseinheit oder verwaltete Einheit), wobei die Erstellung oder Umbenennung von Stammordnern nicht für Benutzerkonten versucht werden soll, die in diesen bestimmten Bereich fallen. In diesem Szenario müssen Sie gewährleisten, dass die Option **Stammverzeichnis auf Dateiserver bei Bedarf erstellen oder umbenennen** im integrierten Richtlinienobjekt aktiviert ist. Dann müssen Sie ein Richtlinienobjekt erstellen und konfigurieren, das eine Richtlinie der Kategorie „Automatische Bereitstellung eines Stammordners" mit deaktivierter Option **Stammverzeichnis auf Dateiserver bei Bedarf erstellen oder umbenennen** enthält, und dieses Richtlinienobjekt dann auf den betreffenden Bereich anwenden.

Konfigurieren der Richtlinie „Einschränkungen bezüglich des Speicherorts von Stammordnern"

Bei der Erstellung von Stammordnern arbeitet ActiveRoles Server im Sicherheitskontext des Dienstkontos, unter dem der Verwaltungsdienst ausgeführt wird. Daher muss das Dienstkonto über ausreichende Rechte zur Erstellung von Stammordnern verfügen. Normalerweise hat das Dienstkonto administrative Rechte für den gesamten Dateiserver, was es ActiveRoles Server ermöglicht, Stammordner in jedem beliebigen Ordner in jeder Netzwerkdateifreigabe zu erstellen, die auf diesem Server existiert. Die Richtlinie „Einschränkung bezüglich des Speicherorts des Stammordners" wird verwendet, um die Netzwerkdateifreigaben und -ordner, in denen ActiveRoles Server Stammordner erstellen darf, auf eine bestimmte Liste zu beschränken.

Die Richtlinie „Einschränkung bezüglich des Speicherorts des Stammordners" legt die Ordner in den Netzwerkdateifreigaben fest, in denen ActiveRoles Server Stammordner erstellen darf, und verhindert, dass ActiveRoles Server Stammordner an anderen Speicherpositionen erstellt. Die von dieser Richtlinie auferlegten Einschränkungen gelten nicht, wenn die Erstellung des Stammordners von einem Inhaber

der Rolle „AR Server Admin" durchgeführt wird (normalerweise sind dies die Benutzer, die Mitglied in der lokalen Administratorengruppe auf dem Computer sind, auf dem der ActiveRoles Server Verwaltungsdienst ausgeführt wird). Wenn als ein Inhaber der Rolle „AR Server Admin" ein Benutzerkonto erstellt und eine bestimmte Richtlinie zur Erleichterung der Bereitstellung von Stammordnern gültig ist, wird der Stammordner unabhängig von den Einstellungen der Richtlinie „Einschränkung bezüglich des Speicherorts des Stammordners" erstellt.

Standardmäßig sind keine Netzwerkdateifreigaben und -ordner in der Richtlinie aufgelistet. Das bedeutet, dass ActiveRoles Server keinen Stammordner erstellen kann, sofern der Benutzerverwaltungsvorgang, der die Erstellung des Stammordners umfasst, nicht von einem Inhaber der Rolle „AR Server Admin" durchgeführt wird. Um delegierten Administratoren die Erstellung von Stammordnern zu ermöglichen, müssen Sie die Richtlinie so konfigurieren, dass sie die Ordner in den Netzwerkdateifreigaben auflistet, in denen die Erstellung von Stammordnern zulässig ist. Führen Sie hierzu das nachfolgend beschriebene Verfahren mit Hilfe der ActiveRoles Server-Konsole aus:

Gehen Sie folgendermaßen vor, um die Richtlinie „Einschränkung bezüglich des Speicherorts des Stammordners" zu konfigurieren:

1. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration | Policies | Administration** und wählen Sie dann **Builtin** unter **Administration**.
2. Doppelklicken Sie im Bereich „Details" auf **Built-in Policy – Home Folder Location Restriction**.
3. Doppelklicken Sie auf der Registerkarte **Richtlinien** auf das Listenelement unter **Richtlinienbeschreibung**.
4. Zeigen Sie auf der Registerkarte **Zulässige Speicherorte** die Liste der Ordner in den Netzwerkdateifreigaben an, in denen die Erstellung von Stammordnern zulässig ist, oder ändern Sie diese Liste.

   Wenn sie einen Ordner zur Liste hinzufügen, geben Sie den UNC-Name des Ordners an. Wenn Sie den Namen in der Form \\<Server>\<Freigabe> angeben, können Stammordner in jedem beliebigen Ordner in der angegebenen Netzwerkdateifreigabe erstellt werden. Wenn Sie den Namen in der Form \\<Server>\<Freigabe>\<PfadZumOrdner> angeben, können Stammordner in jedem beliebigen Unterordner des Ordners in der Netzwerkfreigabe erstellt werden.

Szenario: Erstellen und Zuweisen von Stammordnern

In diesem Szenario konfigurieren Sie eine Richtlinie, mit der bei der Erstellung von Benutzerkonten auch Stammordner erstellt werden. Die Richtlinie weist neu erstellten Konten Stammordner zu und gewährt den Benutzern Änderungszugriff auf ihre Stammordner.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Überprüfen Sie, ob die Netzwerkdateifreigabe, in der die Richtlinie Stammordner erstellen soll, in der Richtlinie Einschränkung bezüglich des Speicherorts des Stammordners aufgelistet ist.
2. Erstellen und konfigurieren Sie ein Richtlinienobjekt, das die entsprechende Richtlinie definiert.
3. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Wenn Sie in dem in Schritt 3 ausgewählten Container ein Benutzerkonto erstellen, erstellt ActiveRoles Server folglich den Benutzerstammordner und weist ihn dem Benutzerkonto zu.

In den folgenden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Überprüfen der Richtlinie „Einschränkung bezüglich des Speicherorts des Stammordners"

Die Netzwerkdateifreigabe, in der sich die Stammordner befinden sollen, muss in der Richtlinie „Einschränkung bezüglich des Speicherorts des Stammordners" aufgeführt sein. Befolgen Sie das Verfahren „Konfigurieren der Richtlinie „Einschränkungen bezüglich des Speicherorts von Stammordnern"", um zu überprüfen, ob die Richtlinie die Erstellung von Stammordnern in der Netzwerkdateifreigabe zulässt.

Schritt 2: Erstellen und Konfigurieren des Richtlinienobjekts

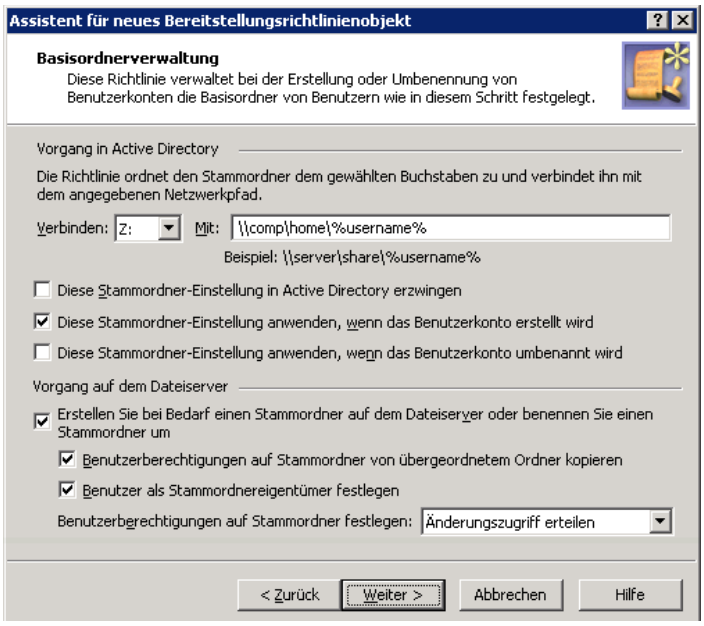
Sie können das benötigte Richtlinienobjekt mit dem Assistenten für neues Bereitstellungsrichtlinien-objekt erstellen und konfigurieren. Weitere Informationen über den Assistenten finden Sie unter „Erstellen eines Richtlinienobjekts" im Abschnitt „Verwaltungsaufgaben für Richtlinienobjekte" weiter oben in diesem Kapitel.

Klicken Sie zum Konfigurieren der Richtlinie auf der Seite **Zu konfigurierende Richtlinie** des Assistenten auf **Automatische Bereitstellung des Stammordners**. Klicken Sie dann auf **Weiter**.

Richten Sie auf der Seite **Basisordnerverwaltung** folgende Optionen ein:

- Wählen Sie im Feld **Verbinden** den Laufwerkbuchstaben aus, der dem Stammordner zugewiesen werden soll. Sie können beispielsweise **Z:** auswählen.
- Geben Sie in das Feld **Mit** den Pfad in der Formular \\Server\Freigabe\%Benutzername% ein, wobei \\Server\Freigabe ein gültiger UNC-Pfad zu einer Netzwerkdateifreigabe ist. Wenn Sie beispielsweise auf dem Server **comp** eine Netzwerkdateifreigabe eingerichtet haben, deren Freigabename auf **home** gesetzt ist, können Sie folgenden Pfad angeben: \\comp\home\%Benutzername%
- Aktivieren Sie das Kontrollkästchen **Diese Stammordner-Einstellung anwenden, wenn das Benutzerkonto erstellt wird**.

Nunmehr sollte die Seite **Basisordnerverwaltung** der folgenden Abbildung entsprechen.


Assistent für neues Bereitstellungsrichtlinienobjekt
Basisordnerverwaltung
Diese Richtlinie verwaltet bei der Erstellung oder Umbenennung von Benutzerkonten die Basisordner von Benutzern wie in diesem Schritt festgelegt.
Vorgang in Active Directory
Die Richtlinie ordnet den Stammordner dem gewählten Buchstaben zu und verbindet ihn mit dem angegebenen Netzwerkpfad.
Verbinden: Z:
Mit: \\comp\home\%username%
Beispiel: \\server\share\%username%
Diese Stammordner-Einstellung in Active Directory erzwingen
Diese Stammordner-Einstellung anwenden, wenn das Benutzerkonto erstellt wird
Diese Stammordner-Einstellung anwenden, wenn das Benutzerkonto umbenannt wird
Vorgang auf dem Dateiserver
Erstellen Sie bei Bedarf einen Stammordner auf dem Dateiserver oder benennen Sie einen Stammordner um
Benutzerberechtigungen auf Stammordner von übergeordnetem Ordner kopieren
Benutzer als Stammordnereigentümer festlegen
Benutzerberechtigungen auf Stammordner festlegen: Änderungszugriff erteilen
< Zurück
Weiter >
Abbrechen
Hilfe

Klicken Sie auf **Weiter** und befolgen Sie die Schritte des Assistenten, um das Richtlinienobjekt zu erstellen.

Schritt 3: Anwenden des Richtlinienobjekts

Sie können das Richtlinienobjekt mit Hilfe der Seite **Richtlinie erzwingen** im Assistenten für neues Bereitstellungsrichtlinienobjekt anwenden oder Sie können den Assistenten erst abschließen und dann den Befehl **Richtlinie erzwingen** für die Domäne, die Organisationseinheit oder die verwaltete Einheit verwenden, auf die Sie die Richtlinie anwenden möchten. Weitere Informationen über die Anwendung eines Richtlinienobjekts finden Sie unter „Anwenden von Richtlinienobjekten" und „Verwalten des Richtlinienbereichs" weiter oben in diesem Kapitel.

Skriptausführung

Richtlinien dieser Kategorie dienen der Ausführung ergänzender Skripts auf Anforderung zur Ausführung administrativer Vorgänge.

Richtlinien, die auf der Ausführung benutzerdefinierter Skripts basieren, können Datenformate und -anforderungen regulieren, Verwaltungsaufgaben automatisieren sowie zusätzliche Aktionen auslösen, um die Kontenbereitstellung zu automatisieren. Sie können ein benutzerdefiniertes Skript einem administrativen Vorgang zuordnen und dem Skript die Kontrolle geben, wenn der Vorgang angefordert wird oder nachdem er abgeschlossen wurde.

Betrachten Sie beispielsweise einen Benutzer, der von Seattle nach Atlanta geht. Sie können ein Skript schreiben, das den Benutzer von der Organisationseinheit Seattle in die Organisationseinheit Atlanta verschiebt, wenn das Attribut für die Stadt im Benutzerkonto aktualisiert wird.

Funktionsweise dieser Richtlinie

ActiveRoles Server führt das in der Richtlinie angegebene Skriptmodul aus, wenn der Vorgang angefordert wird oder nachdem er abgeschlossen wurde. Das Skriptmodul wird in der Konfigurationsdatenbank von ActiveRoles Server gespeichert.

Konfigurieren der Richtlinie „Skriptausführung"

Beim Konfigurieren der Richtlinie „Skriptausführung" können Sie vorab ein Skriptmodul vorbereiten. Alternativ können Sie auch beim Konfigurieren einer Richtlinie ein leeres Skriptmodul erstellen und dieses später bearbeiten, um ein von der Richtlinie zu verwendendes Skript hinzuzufügen.

Sie können ein Skript aus einer Datei importieren oder mit Hilfe der ActiveRoles Server-Konsole ein neues Skript schreiben. Auf der Konsole werden Skriptmodule im Container **Script Modules** unter **Configuration** angezeigt.

Importieren eines Skripts

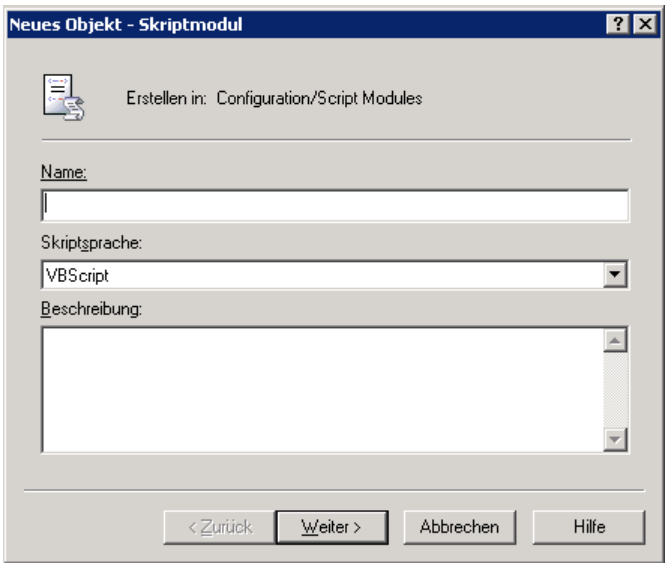
Klicken Sie zum Importieren einer Skriptdatei in der Konsolenstruktur mit der rechten Maustaste auf **Script Modules**, und klicken Sie dann auf **Importieren**. Dann wird das Dialogfeld **Skript importieren** angezeigt, in dem Sie eine Skriptdatei auswählen und öffnen können.

Erstellen eines Skripts

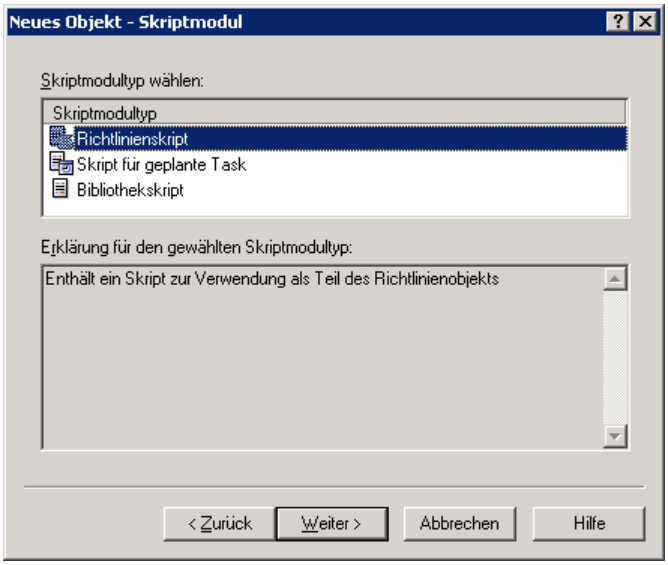
Um ein neues Skriptmodul zu erstellen, klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf **Script Modules** und wählen Sie **Neu | Skriptmodul**. Dann wird der Assistent „Neues Objekt – Skriptmodul" geöffnet.

Sie sollten benutzerdefinierte Skriptmodule in einem separaten Container speichern. Sie können wie folgt einen Container erstellen: Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf **Script Modules** und wählen Sie **Neu | Skriptcontainer**. Nachdem Sie einen Container erstellt haben, können Sie mit Hilfe des Assistenten ein Skriptmodul zu dem Container anstatt direkt zu den **Script Modules** hinzufügen: Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf den Container, und wählen Sie **Neu | Skriptmodul** aus.

Die erste Seite des Assistenten entspricht der folgenden Abbildung.



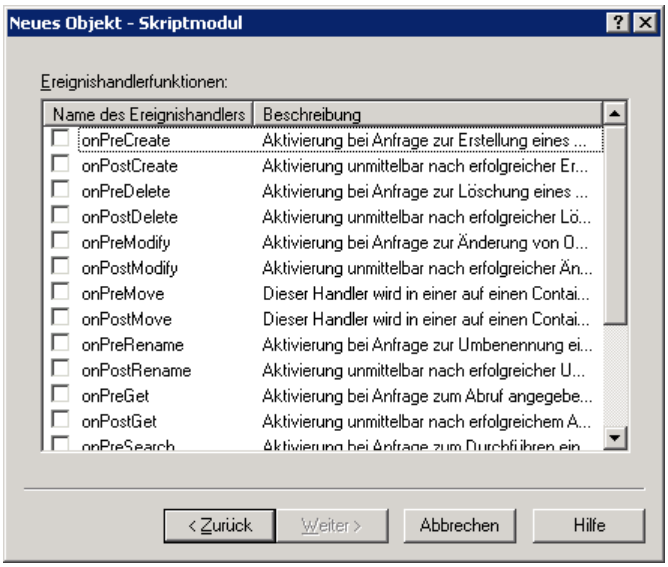
Geben Sie einen Namen und eine Beschreibung für das neue Skriptmodul ein, und wählen Sie die Skriptsprache aus. Klicken Sie dann auf **Weiter**. Die nächste Seite sollte der folgenden Abbildung entsprechen.



Wählen Sie auf dieser Seite einen Skriptmodultyp aus. Wählen Sie **Richtlinienskript** aus, um ein Skript zu erstellen, das als Teil des Richtlinienobjekts verwendet werden soll. Die anderen Optionen lauten:

- **Skript für geplante Task** Ein Skript, für das Sie die Ausführung für den Verwaltungsdienst planen können.
- **Bibliothekskript** Ein Skript, das von anderen Skriptmodulen verwendet werden soll. Sie können häufig verwendete Funktionen in einem eigenständigen Skriptmodul sammeln und es in andere Module einschließen, die diese Funktionen benötigen. So können Sie Teile vorhandener Skripts wieder verwenden und somit Aufwand und Zeit für die Entwicklung reduzieren.

Wählen Sie **Richtlinienskript** aus, und klicken Sie dann auf **Weiter**. Nun wird die in der folgenden Abbildung gezeigte Seite mit einer Liste von Ereignishandlerfunktionen angezeigt.



Wählen Sie auf dieser Seite Funktionen aus, die in dem Skript verwendet werden sollen, und klicken Sie dann auf **Weiter**. Klicken Sie dann auf **Fertig stellen**, um das Skriptmodul zu erstellen.

Anweisungen und Richtlinien für das Entwickeln von Richtlinienskripts finden Sie im ActiveRoles Server Software Development Kit (SDK).

Auf der ActiveRoles Server-Konsole können Sie importierte sowie neu erstellte Skripts anzeigen und ändern.

Bearbeiten eines Skripts

Um ein Skript zu bearbeiten, wählen Sie es in der Konsolenstruktur unter **Configuration/Script Modules** aus. Sie können das Skript im Bereich „Details" anzeigen und ändern. Um die Bearbeitung des Skripts zu beginnen, klicken Sie mit der rechten Maustaste auf das Skriptmodul, und klicken Sie dann auf **Skript bearbeiten**. Klicken Sie dann auf **Ja**, um den Vorgang zu bestätigen. Sie können das Skript im Bereich „Details" ändern.

Wenn Sie das Skript bearbeiten, wird in der Konsolenstruktur neben dem Namen des Skriptmoduls ein rotes Sternchen angezeigt. Dies zeigt an, dass die am Skript vorgenommen Änderungen noch nicht gespeichert wurden. Sie können die Änderungen wie folgt rückgängig machen oder speichern:

- Drücken Sie zum Rückgängigmachen von Änderungen STRG+Z. (Sie können rückgängig gemacht Änderungen auch wiederherstellen: Drücken Sie STRG+Y.)
- Um alle nicht gespeicherten Änderungen rückgängig zu machen, klicken Sie mit der rechten Maustaste auf das Skriptmodul, und klicken Sie dann auf **Änderungen verwerfen**. (Dieser Vorgang ist nicht umkehrbar: Wenn Sie diesen Befehl ausführen, gehen Ihre Änderungen an dem Skript verloren.)
- Um die Änderungen zu speichern, klicken Sie mit der rechten Maustaste auf das Skriptmodul, und klicken Sie dann auf **Skript auf Server speichern**.

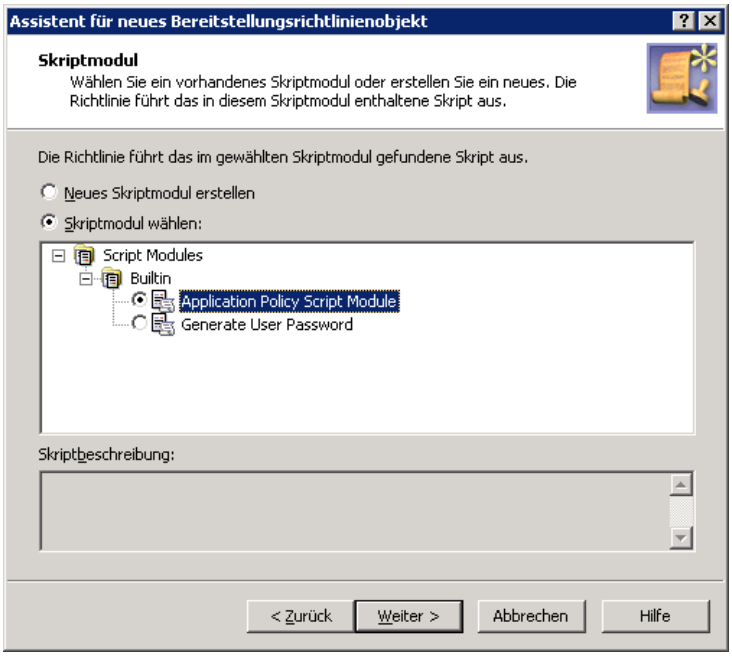
Wenn das Skriptmodul bereit ist, können Sie eine Skriptrichtlinie konfigurieren, die das vorbereitete Skriptmodul verwendet.

Mit ActiveRoles Server können Sie einen Debugger an den Skripthost des Verwaltungsdienstes für ein bestimmtes Richtlinienskript oder geplantes Taskskript anfügen. Wenn das Skript von dem angegebenen Verwaltungsdienst ausgeführt wird, kann der Debugger ggf. beim Identifizieren und Isolieren von Problemen mit der Richtlinie oder dem Task helfen, die bzw. der auf diesem Skript basiert.

Um das Debuggen eines Skripts auf der ActiveRoles Server-Konsole zu aktivieren, zeigen Sie das Dialogfeld **Eigenschaften** für das Skriptmodul an, das das Skript enthält, öffnen Sie die Registerkarte **Fehlerbehebung**, und aktivieren Sie das Kontrollkästchen **Debuggen aktivieren**. Wählen Sie in der Liste **Debug auf Server** den Verwaltungsdienst aus, für den der Debugger ausgeführt werden soll.

Konfigurieren einer Richtlinie zur Ausführung eines Skripts

Um eine skriptbasierte Richtlinie zu konfigurieren, wählen Sie **Skriptausführung** auf der Seite **Richtlinientyp auswählen** im Assistenten für neues Bereitstellungsrichtlinienobjekt oder im Assistenten „Neues Deprovisionsrichtlinienobjekt“ oder im Assistenten „Richtlinie hinzufügen“ aus. Klicken Sie dann auf **Weiter**, damit die Seite **Skriptmodul** angezeigt wird.


Assistent für neues Bereitstellungsrichtlinienobjekt
Skriptmodul
Wählen Sie ein vorhandenes Skriptmodul oder erstellen Sie ein neues. Die Richtlinie führt das in diesem Skriptmodul enthaltene Skript aus.
Die Richtlinie führt das im gewählten Skriptmodul gefundene Skript aus.
Neues Skriptmodul erstellen
Skriptmodul wählen:
Script Modules
Builtin
Application Policy Script Module
Generate User Password
Skriptbeschreibung:
< Zurück
Weiter >
Abbrechen
Hilfe

Klicken Sie auf dieser Seite auf **Skriptmodul wählen**, und wählen Sie das Skriptmodul aus. Klicken Sie dann auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schrittweise Anleitungen finden Sie unter **Anleitungen/Verwalten von Richtlinienobjekten/Konfigurieren von Bereitstellungsrichtlinienobjekten/Konfigurieren einer Skriptausführungsrichtlinie** in der ActiveRoles Server-Hilfe.

Szenario: Einschränken des Verteilergruppentyps

In diesem Szenario wird das Konfigurieren einer Richtlinie beschrieben, mit der sichergestellt wird, dass nur universelle Gruppen für die Verwendung von E-Mail aktiviert werden können. Das Skript verhindert, dass ActiveRoles Server neue für die Verwendung von E-Mail aktivierte, nicht universelle Gruppen erstellt oder vorhandene nicht universelle Gruppen für die Verwendung von E-Mail aktiviert.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Bereiten Sie das Skript vor, mit dem dieses Szenario implementiert wird.
2. Erstellen und konfigurieren Sie das Richtlinienobjekt für die Ausführung dieses Skripts.
3. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Beim Erstellen oder Ändern einer nicht universellen Gruppe in dem in Schritt 3 ausgewählten Container lehnt ActiveRoles Server nunmehr Versuche ab, die Gruppe für die Verwendung von E-Mail zu aktivieren.

In den folgenden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Vorbereiten des Skriptmoduls

Das in diesem Szenario verwendete Skript wird mit dem ActiveRoles Server-Verwaltungsdienst installiert. Standardmäßig lauten der Pfad und Name der Skriptdatei wie folgt: „%Programme%\Quest Software\ActiveRoles Server\SDK\Samples\RestrictDistrGroups\RestrictDistrGroups.vbs"

Das Skript erhält entwurfsgemäß die Kontrolle, wenn Anforderungen eingehen, Gruppen für die Verwendung von E-Mail zu aktivieren. Das Skript überprüft den Typ der Gruppe und lässt den angeforderten Vorgang nur für universelle Gruppen zu. Weitere Informationen zu diesem Skript finden Sie im ActiveRoles Server Software Development Kit (SDK).

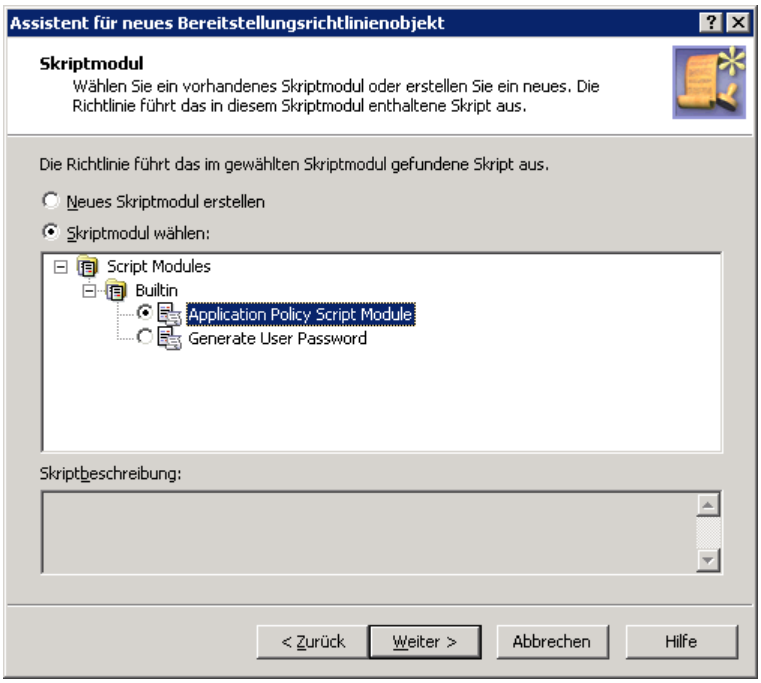
Um das Skript zu importieren, klicken Sie mit der rechten Maustaste auf den Container **Script Modules**, und klicken Sie dann auf **Importieren**. Wählen Sie dann die Datei **RestrictDistrGroups.vbs** aus und öffnen Sie sie.

Schritt 2: Erstellen und Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt mit dem Assistenten für neues Bereitstellungsrichtlinienobjekt erstellen und konfigurieren. Weitere Informationen über den Assistenten finden Sie unter „Erstellen eines Richtlinienobjekts" im Abschnitt „Verwaltungsaufgaben für Richtlinienobjekte" weiter oben in diesem Kapitel.

Klicken Sie zum Konfigurieren der Richtlinie auf der Seite **Zu konfigurierende Richtlinie** des Assistenten auf **Skriptausführung**. Klicken Sie dann auf **Weiter**.

Klicken Sie auf der Seite **Skriptmodul** auf **Skriptmodul wählen**, und wählen Sie in der Liste der Skriptmodule den Eintrag **RestrictDistrGroups** aus, wie in der folgenden Abbildung gezeigt.


Assistent für neues Bereitstellungsrichtlinienobjekt
Skriptmodul
Wählen Sie ein vorhandenes Skriptmodul oder erstellen Sie ein neues. Die Richtlinie führt das in diesem Skriptmodul enthaltene Skript aus.
Die Richtlinie führt das im gewählten Skriptmodul gefundene Skript aus.
Neues Skriptmodul erstellen
Skriptmodul wählen:
Script Modules
Builtin
Application Policy Script Module
Generate User Password
Skriptbeschreibung:
< Zurück
Weiter >
Abbrechen
Hilfe

Klicken Sie auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schritt 3: Anwenden des Richtlinienobjekts

Sie können das Richtlinienobjekt mit Hilfe der Seite **Richtlinie erzwingen** im Assistenten für neues Bereitstellungsrichtlinienobjekt anwenden oder Sie können den Assistenten erst abschließen und dann den Befehl **Richtlinie erzwingen** für die Domäne, die Organisationseinheit oder die verwaltete Einheit verwenden, auf die Sie die Richtlinie anwenden möchten.

Weitere Informationen über die Anwendung eines Richtlinienobjekts finden Sie unter „Anwenden von Richtlinienobjekten“ und „Verwalten des Richtlinienbereichs“ weiter oben in diesem Kapitel.

Benutzerkontodeprovisionierung

Richtlinien dieser Kategorie dienen zum Automatisieren der folgenden Aufgaben im Zusammenhang mit dem Zurücknehmen der Bereitstellung für Benutzerkonten:

- Deaktivieren des Benutzerkontos
- Festlegen des Benutzerkennworts auf einen zufälligen Wert
- Festlegen der Anmeldenamen des Benutzers auf zufällige Werte
- Umbenennen des Benutzerkontos
- Ändern anderer Eigenschaften des Benutzerkontos

Wenn Sie eine Richtlinie dieser Kategorie konfigurieren, geben Sie an, wie ActiveRoles Server bei einer Deprovisionsanforderung für einen Benutzer das Konto des Benutzers in Active Directory ändern soll. Der Deprovisionsvorgang muss dazu führen, dass der Benutzer sich nicht mehr am Netzwerk anmelden kann.

Sie können auch eine Richtlinie so konfigurieren, dass sie beliebige Benutzereigenschaften aktualisiert, z.B., die, die die Mitgliedschaft von Benutzern in verwalteten Einheiten von ActiveRoles Server regulieren. So kann die Richtlinie das Hinzufügen oder Entfernen von Benutzern, für die die Bereitstellung zurückgenommen wird, aus verwalteten Einheiten automatisieren.

Funktionsweise dieser Richtlinie

Beim Verarbeiten einer Deprovisionsanforderung für einen Benutzer verwendet ActiveRoles Server diese Richtlinie, um das Konto des Benutzers so zu ändern, dass dieser Benutzer sich nicht mehr am Netzwerk anmelden kann.

Es kann auch eine Richtlinie zum Aktualisieren von Benutzerkonten konfiguriert werden. Abhängig von der Richtlinienkonfiguration hat jede richtlinienbasierte Aktualisierung folgende Ergebnisse:

- Bestimmte Teile von Kontoinformationen werden aus dem Verzeichnis entfernt, indem bestimmte Eigenschaften auf „leere" Werte zurückgesetzt werden.
- Bestimmte Eigenschaften von Benutzerkonten werden auf neue, nicht leere Werte zurückgesetzt.

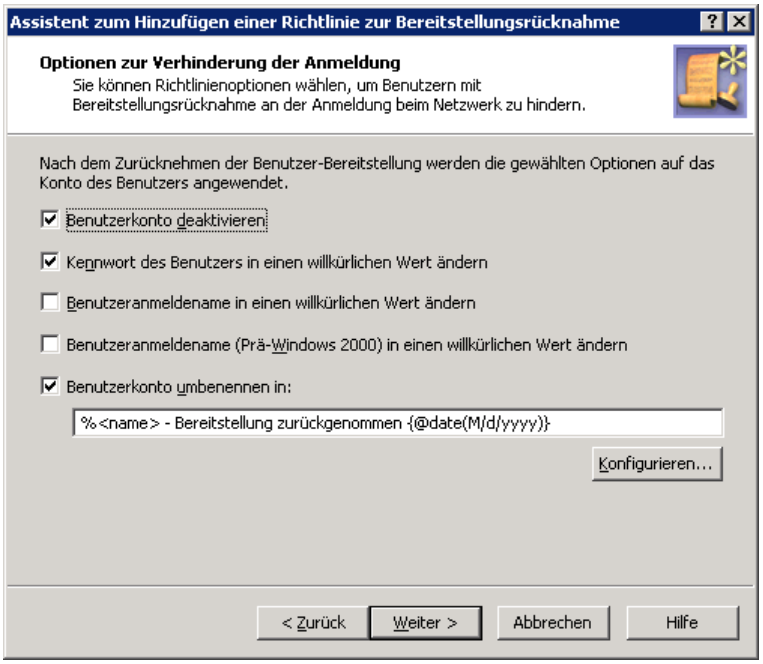
Eine Richtlinie kann so konfiguriert werden, dass sie folgende neue Eigenschaftswerte einschließt:

- Eigenschaften des Benutzerkontos, für das die Bereitstellung zurückgenommen wird. Diese Eigenschaften wurden vor dem Beginn des Rücknahmevorgangs für den Benutzer aus dem Verzeichnis abgerufen
- Eigenschaften des Benutzers, der die Rücknahmeanforderung gestellt hat
- Datum und Uhrzeit der Deprovision für den Benutzer

ActiveRoles Server ändert also bei der Deprovision für einen Benutzer das Benutzerkonto in Active Directory so, wie es von der gültigen Richtlinie „Benutzerkontodeprovisionierung" bestimmt wird.

Konfigurieren der Richtlinie „Benutzerkontodeprovisionierung“

Um die Richtlinie „Benutzerkontodeprovisionierung“ zu konfigurieren, wählen Sie **Benutzerkonto-deprovisionierung** auf der Seite **Zu konfigurierende Richtlinie** im Assistenten „Neues Deprovisions-richtlinienobjekt“ oder im Assistenten „Deprovisionsrichtlinie hinzufügen“ aus. Klicken Sie dann auf **Weiter**, damit die Seite **Optionen zur Verhinderung der Anmeldung** angezeigt wird.


Assistent zum Hinzufügen einer Richtlinie zur Bereitstellungsrücknahme
Optionen zur Verhinderung der Anmeldung
Sie können Richtlinienoptionen wählen, um Benutzern mit Bereitstellungsrücknahme an der Anmeldung beim Netzwerk zu hindern.
Nach dem Zurücknehmen der Benutzer-Bereitstellung werden die gewählten Optionen auf das Konto des Benutzers angewendet.
Benutzerkonto deaktivieren
Kennwort des Benutzers in einen willkürlichen Wert ändern
Benutzeranmeldename in einen willkürlichen Wert ändern
Benutzeranmeldename (Prä-Windows 2000) in einen willkürlichen Wert ändern
Benutzerkonto umbenennen in:
%<name> - Bereitstellung zurückgenommen {@date(M/d/yyyy)}
Konfigurieren...
< Zurück
Weiter >
Abbrechen
Hilfe

Auf dieser Seite können Sie Optionen auswählen, die Anmeldungen mit diesem Konto verhindern. Die Optionsnamen sind selbsterklärend:

- Deaktivieren des Benutzerkontos
- Festlegen des Kennworts des Benutzers auf einen zufälligen Wert
- Festlegen des Anmeldenamens des Benutzers auf einen zufälligen Wert
- Festlegen des Benutzer-Anmeldenamens (Prä-Windows 2000) auf einen zufälligen Wert

Aktivieren Sie die Kontrollkästchen neben den Optionen, die die Richtlinie anwenden soll.

Durch Aktivieren des Kontrollkästchens **Benutzerkonto umbenennen in** weisen Sie die Richtlinie an, den Benutzernamen des Kontos zu ändern. Mit dieser Option können Sie eine *Eigenschafts-aktualisierungsregel* konfigurieren, die angibt, wie der Benutzername geändert werden soll. Im folgenden Unterabschnitt werden Anweisungen zum Konfigurieren einer Eigenschaftsaktualisierungs-regel bereitgestellt. Dabei wird der Benutzername als Beispiel verwendet.

Konfigurieren einer Eigenschaftsaktualisierungsregel

Um eine Eigenschaftsaktualisierungsregel für den Benutzernamen zu konfigurieren, klicken Sie auf die Schaltfläche **Konfigurieren**. Hierdurch wird das Dialogfeld **Wert konfigurieren** geöffnet, das weiter oben in diesem Kapitel beschrieben wurde (siehe „Konfigurieren einer Richtlinie für die Generierung und Validierung von Eigenschaften“). In diesem Dialogfeld können Sie einen Wert für die Bedingung **„Name“ muss sein** konfigurieren, ähnlich wie beim Konfigurieren der Richtlinie „Erzeugung und Validierung von Eigenschaften“.

Um mit dem Konfigurieren eines Wertes zu beginnen, klicken Sie im Dialogfeld **Wert konfigurieren** auf **Hinzufügen**. Nun wird das Fenster **Eintrag hinzufügen** angezeigt.

Ein Wert entsteht durch Verkettung von mindestens einem Eintrag. Im Fenster **Eintrag hinzufügen** können Sie den Typ des hinzuzufügenden Eintrags auswählen und den Eintrag dann konfigurieren. In der folgenden Tabelle werden die verfügbaren Eintragstypen zusammengefasst.

EINTRAGSTYP	BESCHREIBUNG
Text	Fügt dem Wert eine Textzeichenfolge hinzu.
Benutzereigenschaft	Fügt eine ausgewählte Eigenschaft (oder einen Teil einer Eigenschaft) des Benutzerkontos hinzu, für das die Bereitstellung zurückgenommen wird.
Eigenschaft der übergeordneten Organisationseinheit	Fügt eine ausgewählte Eigenschaft (oder einen Teil einer Eigenschaft) einer Organisationseinheit in der Containerhierarchie über dem Benutzerkonto hinzu, für das die Bereitstellung zurückgenommen wird.
Eigenschaft der übergeordneten Domäne	Fügt eine ausgewählte Eigenschaft (oder einen Teil einer Eigenschaft) der Domäne des Benutzerkontos hinzu, für das die Bereitstellung zurückgenommen wird.
Datum und Uhrzeit	Zeigt das Datum und die Uhrzeit der Deprovision für das Konto an.
Initiator-ID	Fügt eine Zeichenfolge hinzu, die den Initiator identifiziert, d.h. den Benutzer, der die Rücknahmeanforderung gestellt hat. Dieser Eintrag besteht aus Eigenschaften, die im Zusammenhang mit dem Initiator stehen und die aus dem Verzeichnis abgerufen wurden.

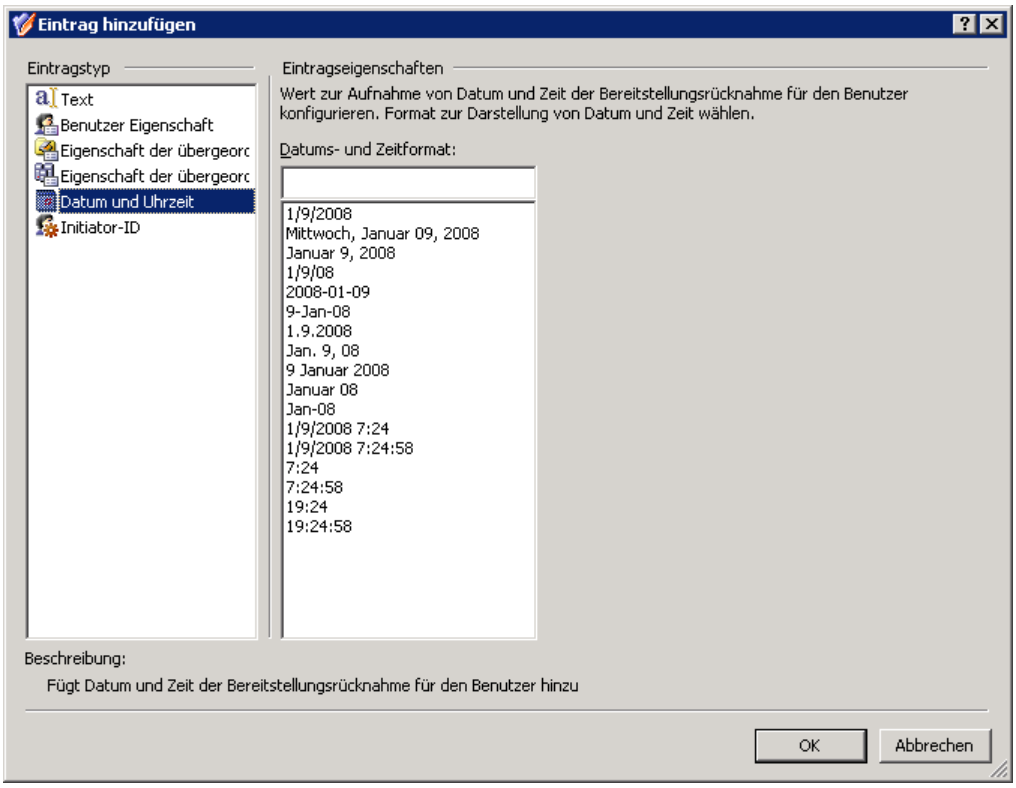
Die Anweisungen zum Konfigurieren eines Eintrags hängen vom Eintragstyp ab. Gehen Sie gemäß den Anweisungen vor, die im Abschnitt „Konfigurieren einer Richtlinie für die Generierung und Validierung von Eigenschaften" weiter oben in diesem Kapitel aufgeführt sind, um einen Eintrag eines dieser Typen zu konfigurieren:

- **Text** Siehe Unterabschnitt „Eintragstyp: Text".
- **Benutzereigenschaft** Siehe Unterabschnitt „Eintragstyp: <Objekt> Eigenschaft".
- **Eigenschaft der übergeordneten Organisationseinheit** Siehe Unterabschnitt „Eintragstyp: Eigenschaft der übergeordneten Organisationseinheit".
- **Eigenschaft der übergeordneten Domäne** Siehe Unterabschnitt „Eintragstyp: Eigenschaft der übergeordneten Domäne".

In den folgenden Unterabschnitten werden die Einträge **Datum und Uhrzeit** und **Initiator-ID** erörtert.

Eintragstyp: Datum und Uhrzeit

Wenn Sie im Fenster **Eintrag hinzufügen** unter **Eintragstyp** den Typ **Datum und Uhrzeit** auswählen, ähnelt der Bereich **Eintragseigenschaften** der folgenden Abbildung.

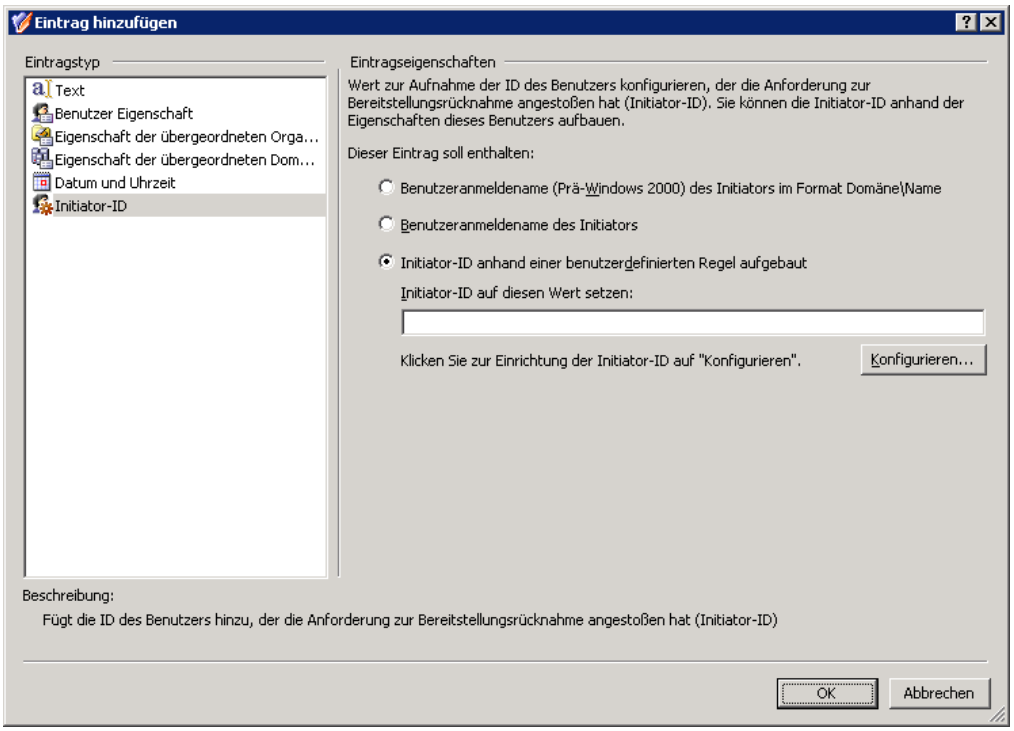


Durch die Verwendung dieses Eintragstyps können Sie einen Eintrag hinzufügen, der das Datum und die Uhrzeit der Deprovision für das Benutzerkonto darstellt.

Klicken Sie in der Liste unter **Datums- und Zeitformat** auf das gewünschte Datums- oder Uhrzeitformat. Klicken Sie dann auf **OK**, um das Fenster **Eintrag hinzufügen** zu schließen.

Eintragstyp: Initiator-ID

Wenn Sie im Fenster **Eintrag hinzufügen** unter **Eintragstyp** den Typ **Initiator-ID** auswählen, ähnelt der Bereich **Eintragseigenschaften** der folgenden Abbildung.


Eintrag hinzufügen
Eintragstyp
Text
Benutzer Eigenschaft
Eigenschaft der übergeordneten Orga...
Eigenschaft der übergeordneten Dom...
Datum und Uhrzeit
Initiator-ID
Eintragseigenschaften
Wert zur Aufnahme der ID des Benutzers konfigurieren, der die Anforderung zur Bereitstellungsrücknahme angestoßen hat (Initiator-ID). Sie können die Initiator-ID anhand der Eigenschaften dieses Benutzers aufbauen.
Dieser Eintrag soll enthalten:
Benutzeranmeldename (Prä-Windows 2000) des Initiators im Format Domäne\Name
Benutzeranmeldename des Initiators
Initiator-ID anhand einer benutzerdefinierten Regel aufgebaut
Initiator-ID auf diesen Wert setzen:
Klicken Sie zur Einrichtung der Initiator-ID auf "Konfigurieren".
Konfigurieren...
Beschreibung:
Fügt die ID des Benutzers hinzu, der die Anforderung zur Bereitstellungsrücknahme angestoßen hat (Initiator-ID)
OK
Abbrechen

Mit diesem Eintragstyp können Sie eine Zeichenfolge hinzufügen, die den Initiator identifiziert, d.h. den Benutzer, der die Rücknahmeanforderung gestellt hat. Die Richtlinie generiert die Initiator-ID anhand bestimmter Kontoeigenschaften des Initiators, z.B. anhand des Benutzer-Anmeldenamens. Zum Verwenden anderer Eigenschaften kann eine benutzerdefinierte Regel konfiguriert werden.

Sie können eine vorkonfigurierte Regel auswählen oder eine benutzerdefinierte Regel konfigurieren, um die Initiator-ID zu generieren. Die vorkonfigurierten Regeln ermöglichen Ihnen, die Initiator-ID auf einen der folgenden Werte zu setzen:

- Den Benutzer-Anmeldenamen (Prä-Windows 2000) des Initiators in der Form *Domänenname**Benutzername*
- Den Benutzer-Anmeldenamen des Initiators

Mit einer benutzerdefinierten Regel können Sie die Initiator-ID aus anderen auf den Initiator bezogenen Eigenschaften zusammensetzen.

Konfigurieren einer benutzerdefinierten Regel zum Erstellen der Initiator-ID

Klicken Sie zum Konfigurieren einer benutzerdefinierten Regel für die Initiator-ID auf die unterste Option unter **Eintragseigenschaften**, und klicken Sie dann auf die Schaltfläche **Konfigurieren**. Hierdurch wird das Dialogfeld **Wert konfigurieren** geöffnet, das weiter oben in diesem Kapitel beschrieben wurde (siehe „Konfigurieren einer Richtlinie für die Generierung und Validierung von Eigenschaften“). In diesem Dialogfeld können Sie einen Wert für die Bedingung **„Initiator-ID“ muss sein** konfigurieren, ähnlich wie beim Konfigurieren der Richtlinie „Erzeugung und Validierung von Eigenschaften“.

Um mit dem Konfigurieren eines Wertes zu beginnen, klicken Sie im Dialogfeld **Wert konfigurieren** auf **Hinzufügen**. Nun wird das Fenster **Eintrag hinzufügen** angezeigt.

Ein Wert entsteht durch Verkettung von mindestens einem Eintrag. Im Fenster **Eintrag hinzufügen** können Sie den Typ des hinzuzufügenden Eintrags auswählen und den Eintrag dann konfigurieren. In der folgenden Tabelle werden die verfügbaren Eintragstypen zusammengefasst.

EINTRAGSTYP	BESCHREIBUNG
Text	Fügt dem Wert eine Textzeichenfolge hinzu.
Eigenschaft des Initiators	Fügt eine ausgewählte Eigenschaft (oder einen Teil einer Eigenschaft) des Benutzerkontos des Initiators hinzu.
Eigenschaft der übergeordneten Organisationseinheit	Fügt eine ausgewählte Eigenschaft (oder einen Teil einer Eigenschaft) einer Organisationseinheit in der Containerhierarchie über dem Benutzerkonto des Initiators hinzu.
Eigenschaft der übergeordneten Domäne	Fügt eine ausgewählte Eigenschaft (oder einen Teil einer Eigenschaft) der Domäne des Benutzerkontos des Initiators hinzu.

Die Anweisungen zum Konfigurieren eines Eintrags hängen vom Eintragstyp ab. Sie finden Anweisungen für jeden Eintragstyp weiter oben in diesem Kapitel:

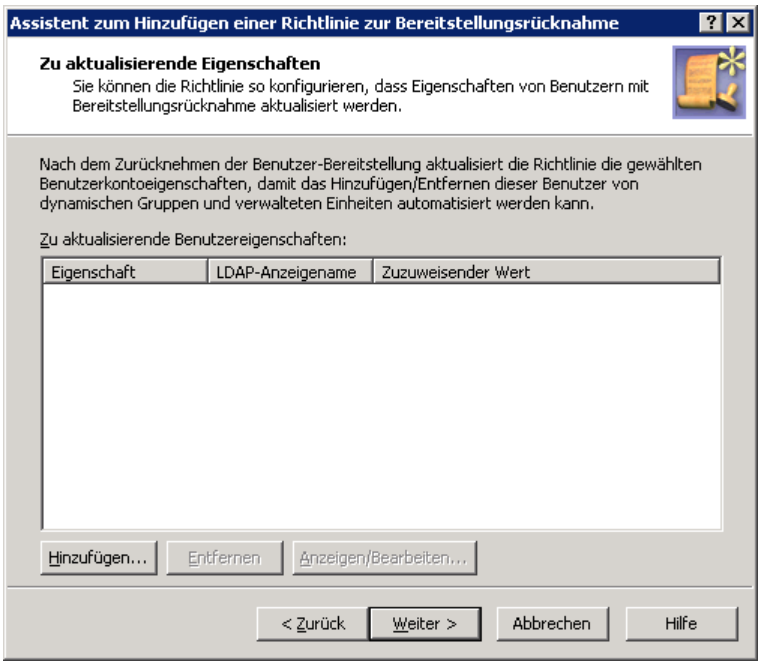
- **Text** Siehe Unterabschnitt „Eintragstyp: Text" im Abschnitt „Konfigurieren der Richtlinie „Erzeugung und Validierung von Eigenschaften"".
- **Eigenschaft des Initiators** Siehe Unterabschnitt „Eintragstyp: <Objekt> Eigenschaft" im Abschnitt „Konfigurieren der Richtlinie „Erzeugung und Validierung von Eigenschaften"".
- **Eigenschaft der übergeordneten Organisationseinheit** Siehe Unterabschnitt „Eintragstyp: Eigenschaft der übergeordneten Organisationseinheit" im Abschnitt „Konfigurieren der Richtlinie „Erzeugung und Validierung von Eigenschaften"".
- **Eigenschaft der übergeordneten Domäne** Siehe Unterabschnitt „Eintragstyp: Eigenschaft der übergeordneten Domäne" im Abschnitt „Konfigurieren der Richtlinie „Erzeugung und Validierung von Eigenschaften"".

Klicken Sie nach dem Konfigurieren eines Wertes für die Bedingung **„Initiator-ID" muss sein** auf **OK**, um das Dialogfeld **Wert konfigurieren** zu schließen. Damit wird der Wert den Eintragseigenschaften für die Initiator-ID hinzugefügt. Nötigenfalls können Sie den Wert ändern. Klicken Sie dazu im Fenster **Eintrag hinzufügen** auf die Schaltfläche **Konfigurieren**, und verwalten Sie dann im Dialogfeld **Wert konfigurieren** die Liste der Einträge.

Klicken Sie nach dem Konfigurieren des Eintrags **Initiator-ID** auf **OK**, um das Fenster **Eintrag hinzufügen** zu schließen. Der Eintrag wird dem Dialogfeld **Wert konfigurieren** für die Bedingung **„Name" muss sein** hinzugefügt.

Klicken Sie nach dem Konfigurieren eines Wertes für die Bedingung **„Name" muss sein** auf **OK**, um das Dialogfeld **Wert konfigurieren** zu schließen. Nun wird die Regel der Seite **Optionen zur Verhinderung der Anmeldung** des Assistenten hinzugefügt. Nötigenfalls können Sie die Regel ändern. Klicken Sie dazu auf die Schaltfläche **Konfigurieren**, und verwalten Sie dann die Liste der Einträge im Dialogfeld **Wert konfigurieren**.

Sobald Sie die Seite **Optionen zur Verhinderung der Anmeldung** abgeschlossen haben, klicken Sie auf **Weiter**, um die Seite **Zu aktualisierende Eigenschaften** anzuzeigen:


Assistent zum Hinzufügen einer Richtlinie zur Bereitstellungsrücknahme
Zu aktualisierende Eigenschaften
Sie können die Richtlinie so konfigurieren, dass Eigenschaften von Benutzern mit Bereitstellungsrücknahme aktualisiert werden.
Nach dem Zurücknehmen der Benutzer-Bereitstellung aktualisiert die Richtlinie die gewählten Benutzerkontoeigenschaften, damit das Hinzufügen/Entfernen dieser Benutzer von dynamischen Gruppen und verwalteten Einheiten automatisiert werden kann.
Zu aktualisierende Benutzereigenschaften:
Eigenschaft
LDAP-Anzeigename
Zuzuweisender Wert
Hinzufügen...
Entfernen
Anzeigen/Bearbeiten...
< Zurück
Weiter >
Abbrechen
Hilfe

Auf dieser Seite können Sie eine Liste von Benutzereigenschaften einrichten, die die Richtlinie aktualisieren soll. Jeder Eintrag in der Liste schließt die folgenden Informationen ein:

- **Eigenschaft** Bei der Deprovision für einen Benutzer aktualisiert ActiveRoles Server diese Eigenschaft des Benutzerkontos.
- **LDAP-Anzeigename** Identifiziert die zu aktualisierende Eigenschaft eindeutig.
- **Zuzuweisender Wert** Nach dem Abschluss des Deprovisionsvorgangs besitzt die Eigenschaft den durch diese Syntax definierten Wert.

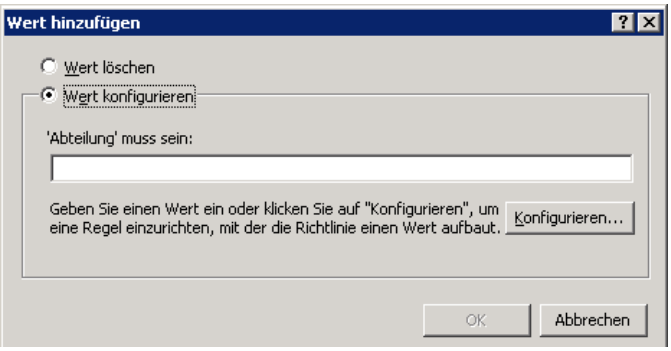
Sie können die Liste auf dieser Seite mit folgenden Schaltflächen verwalten:

- **Hinzufügen** Ermöglicht das Auswählen einer Benutzereigenschaft und das Konfigurieren einer Aktualisierungsregel für diese Eigenschaft. Eine Eigenschaftsaktualisierungsregel gibt an, wie der neue Wert generiert werden soll, der der Eigenschaft zugewiesen wird.
- **Entfernen** Wenn die Richtlinie eine bestimmte Eigenschaft nicht mehr aktualisieren soll, wählen Sie die Eigenschaft in der Liste aus und klicken Sie auf **Entfernen**.
- **Anzeigen/Bearbeiten** Ermöglicht das Ändern der Aktualisierungsregel für die Eigenschaft, die Sie in der Liste auswählen.

Wenn Sie auf die Schaltfläche **Hinzufügen** klicken, wird das Dialogfeld **Objekteigenschaft wählen** angezeigt. In diesem können Sie Benutzereigenschaften auswählen, die die Richtlinie aktualisieren soll. Um eine Eigenschaft auszuwählen, aktivieren Sie das Kontrollkästchen neben dem Eigenschaftsnamen und klicken Sie dann auf **OK**.

Sie können mehrere Kontrollkästchen aktivieren. In diesem Fall werden die ausgewählten Eigenschaften der Liste auf der Seite des Assistenten hinzugefügt, und die Aktualisierungsregel wird so konfiguriert, dass sie diese Eigenschaften löscht, ihnen also den „leeren" Wert zuweist.

Wenn Sie eine einzelne Eigenschaft im Dialogfeld **Objekteigenschaft auswählen** auswählen, wird das Dialogfeld **Wert hinzufügen** angezeigt, sodass Sie den Vorgang mit der Konfiguration einer Eigenschafts-Aktualisierungsregel fortsetzen können:


Wert hinzufügen
Wert löschen
Wert konfigurieren
'Abteilung' muss sein:
Geben Sie einen Wert ein oder klicken Sie auf "Konfigurieren", um eine Regel einzurichten, mit der die Richtlinie einen Wert aufbaut.
Konfigurieren...
OK
Abbrechen

Sie können eine der folgenden Aktualisierungsoptionen auswählen:

- **Wert löschen** Veranlasst die Richtlinie dazu, der Eigenschaft den „leeren" Wert zuzuweisen.
- **Wert konfigurieren** Ermöglicht das Konfigurieren eines Wertes für die Bedingung **„Eigenschaft" muss sein**.

Bei der zweiten Option müssen Sie einen Wert konfigurieren, den die Richtlinie bei der Deprovision für einen Benutzer der Eigenschaft zuweisen soll. Sie können einen Wert auf die gleiche Weise konfigurieren wie beim Konfigurieren einer Eigenschaftsaktualisierungsregel für den Benutzernamen: Klicken Sie auf die Schaltfläche **Konfigurieren** und befolgen Sie die weiter oben in diesem Abschnitt aufgeführten Anleitungen (siehe „Konfigurieren einer Eigenschaftsaktualisierungsregel").

Klicken Sie nach dem Konfigurieren eines Wertes auf **OK**, um das Dialogfeld **Wert hinzufügen** zu schließen. Der Eigenschaftsname wird zusammen mit der Eigenschaftsaktualisierungsregel der Seite des Assistenten hinzugefügt. Nötigenfalls können Sie die Aktualisierungsregel ändern, indem Sie unter der Eigenschaftenliste auf die Schaltfläche **Anzeigen/Bearbeiten** klicken. Dann wird ein Dialogfeld angezeigt, das dem Dialogfeld **Wert hinzufügen** ähnelt und in dem Sie eine andere Aktualisierungsoption auswählen oder einen anderen Wert für die Bedingung **„Eigenschaft" muss sein** festlegen können.

Klicken Sie nach dem Einrichten der Liste auf der Seite des Assistenten auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schrittweise Anleitungen finden Sie unter **Anleitungen/Verwalten von Richtlinienobjekten/ Konfigurieren von Deprovisionsrichtlinienobjekten/Konfigurieren einer Benutzerkonto-Deprovisionierungsrichtlinie** in der ActiveRoles Server-Hilfe.

Szenario 1: Deaktivieren und Umbenennen von Benutzerkonten bei der Deprovision für einen Benutzer

Die in diesem Szenario beschriebene Richtlinie führt während der Deprovision für einen Benutzer die folgenden Funktionen aus:

- Deaktivieren des Benutzerkontos.
- Anhängen des folgenden Suffixes an den Benutzernamen: **- Deprovisioniert**, gefolgt von dem Datum, an dem die Bereitstellung für das Benutzerkonto zurückgenommen wurde.

Beispielsweise ändert die Richtlinie den Benutzernamen **John Smith** in **John Smith – Deprovisioniert am 12/11/2004**.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen und konfigurieren Sie das Richtlinienobjekt, das die entsprechende Richtlinie definiert.
2. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Bei der Deprovision für ein Benutzerkonto in dem Container, den Sie in Schritt 2 ausgewählt haben, deaktiviert ActiveRoles Server folglich das Benutzerkonto und benennt es um, wie von dieser Richtlinie vorgeschrieben.

In den folgenden beiden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen und Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt mit dem Assistenten „Neues Deprovisionsrichtlinienobjekt" erstellen und konfigurieren. Weitere Informationen über den Assistenten finden Sie unter „Erstellen eines Richtlinienobjekts" im Abschnitt „Verwaltungsaufgaben für Richtlinienobjekte" weiter oben in diesem Kapitel.

Klicken Sie zum Konfigurieren der Richtlinie auf der Seite **Richtlinientyp auswählen** des Assistenten auf **Benutzerkontodeprovisionierung**. Klicken Sie dann auf **Weiter**.

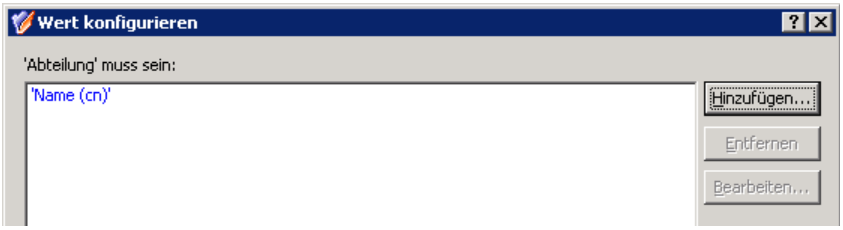
Aktivieren Sie auf der Seite **Optionen zur Verhinderung der Anmeldung** die folgenden Kontrollkästchen:

- **Deaktivieren des Benutzerkontos**
- **Benutzerkonto umbenennen in**

Klicken Sie dann auf die Schaltfläche **Konfigurieren**, und schließen Sie das Dialogfeld **Wert konfigurieren** anhand der folgenden Anweisungen ab.

1. Klicken Sie auf **Hinzufügen**.
2. Klicken Sie im Fenster **Eintrag hinzufügen** unter **Eintragstyp** auf **Benutzereigenschaft**, und konfigurieren Sie den Eintrag wie folgt:
   a) Klicken Sie auf **Auswählen**, und wählen Sie die Eigenschaft **Name** aus.
   b) Klicken Sie auf **Alle Zeichen des Eigenschaftswerts**.
   c) Klicken Sie auf **OK**.
3. Klicken Sie auf **Hinzufügen**.
4. Klicken Sie im Fenster **Eintrag hinzufügen** unter **Eintragstyp** auf **Text**, und konfigurieren Sie den Eintrag wie folgt:
   a) Geben Sie in das Feld **Textwert** den Wert **Deprovisioniert** ein.
   b) Klicken Sie auf **OK**.
5. Klicken Sie auf **Hinzufügen**.
6. Klicken Sie im Fenster **Eintrag hinzufügen** unter **Eintragstyp** auf **Datum und Uhrzeit**, und konfigurieren Sie den Eintrag wie folgt:
   a) Wählen Sie in der Liste unter **Datums- und Zeitformat** das Format **M/T/JJJJ** aus.
   b) Klicken Sie auf **OK**.

Nach dem Ausführen dieser Schritte sollte die Liste der Einträge im Dialogfeld **Wert konfigurieren** der folgenden Abbildung ähneln.



Klicken Sie auf **OK**, um das Dialogfeld **Wert konfigurieren** zu schließen. Klicken Sie dann auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schritt 2: Anwenden des Richtlinienobjekts

Sie können das Richtlinienobjekt mit Hilfe der Seite **Richtlinie erzwingen** im Assistenten „Neues Deprovisionsrichtlinienobjekt" anwenden oder Sie können den Assistenten erst abschließen und dann den Befehl **Richtlinie erzwingen** für die Domäne, die Organisationseinheit oder die verwaltete Einheit verwenden, auf die Sie die Richtlinie anwenden möchten.

Weitere Informationen über die Anwendung eines Richtlinienobjekts finden Sie unter „Anwenden von Richtlinienobjekten" und „Verwalten des Richtlinienbereichs" weiter oben in diesem Kapitel.

Szenario 2: Verwaltete Einheit zum Ablegen deprovisionierter Benutzerkonten

In diesem Szenario wird beschrieben, wie Sie eine verwaltete Einheit und die Richtlinie „Benutzerkonto-deprovisionierung" so konfigurieren, dass die verwaltete Einheit alle deprovisionierten Benutzerkonten enthält. Die Richtlinie legt bei der Deprovision für einen Benutzer die Eigenschaft **Hinweise** auf **Deprovisioniert** fest. Die verwaltete Einheit wiederum ist so konfiguriert, dass sie Benutzerkonten einschließt, deren Eigenschaft **Hinweise** auf **Deprovisioniert** festgelegt ist.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen und konfigurieren Sie die verwaltete Einheit.
2. Konfigurieren Sie das Richtlinienobjekt, das die entsprechende Richtlinie definiert.
3. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Nach der Deprovision für ein Benutzerkonto in dem Container, den Sie in Schritt 3 ausgewählt haben, fügt ActiveRoles Server folglich dieses Konto automatisch der in Schritt 1 erstellten verwalteten Einheit hinzu.

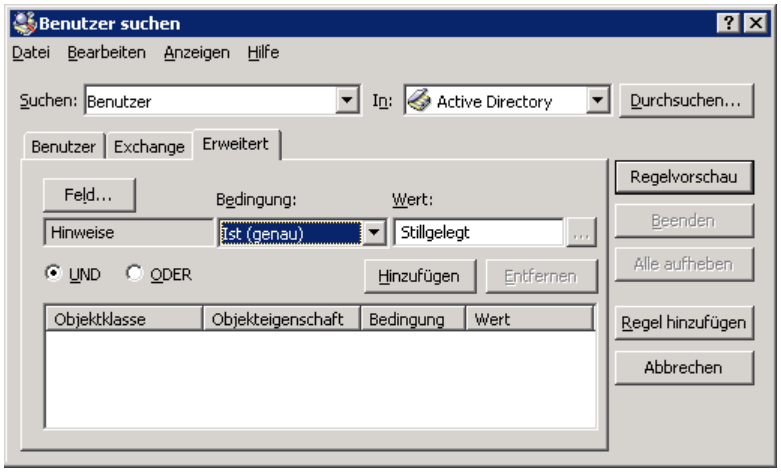
In den folgenden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen und Konfigurieren der verwalteten Einheit

Sie können die verwaltete Einheit mittels der ActiveRoles Server-Konsole erstellen und konfigurieren:

1. Klicken Sie in der Konsolenstruktur unter **Configuration** mit der rechten Maustaste auf **Verwaltete Einheiten**, und wählen Sie **Neu | Verwaltete Einheit** aus.
2. Geben Sie in das Feld **Name** einen Namen für die verwaltete Einheit ein. Sie können beispielsweise **Deprovisionierte Benutzer** eingeben.
3. Klicken Sie auf **Weiter**.
4. Konfigurieren Sie wie folgt die Mitgliedschaftsregel so, dass die verwaltete Einheit die deprovisionierten Benutzerkonten aus allen bei ActiveRoles Server registrierten Domänen (den verwalteten Domänen) enthält:
   a) Klicken Sie auf der Seite des Assistenten auf **Hinzufügen**.
   b) Klicken Sie im Dialogfeld **Mitgliedschaftsregeltyp** auf **Nach Abfrage einschließen** und klicken Sie dann auf **OK**.
   c) Richten Sie im Fenster **Mitgliedschaftsregel erstellen** die Regel ein:
      - Klicken Sie unter **Suchen** auf **Benutzer**.
      - Klicken Sie auf **Durchsuchen** und wählen Sie **Active Directory** aus.
      - Klicken Sie auf die Registerkarte **Erweitert**.
      - Klicken Sie auf die Schaltfläche **Feld** und dann auf **Hinweise**.
      - Klicken Sie unter **Bedingung** auf **Ist (genau)**.
      - Geben Sie unter **Wert** den Wert **Deprovisioniert** ein.

   Nun sollte das Fenster der folgenden Abbildung entsprechen:



   - Klicken Sie auf die Schaltfläche **Hinzufügen**.
   - Klicken Sie auf die Schaltfläche **Regel hinzufügen**.

   d) Klicken Sie auf der Seite des Assistenten auf **Hinzufügen**.
   e) Klicken Sie im Dialogfeld **Mitgliedschaftsregeltyp** auf **Deprovisionierte beibehalten** und klicken Sie dann auf **OK**.
5. Klicken Sie auf **Weiter**, wiederum auf **Weiter** und dann auf **Fertig stellen**.

Schritt 2: Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt konfigurieren, indem Sie das Richtlinienobjekt ändern, das das vorige Szenario implementiert; siehe „Szenario 1: Deaktivieren und Umbenennen von Benutzerkonten bei einer Benutzerdeprovisionierung" weiter oben in diesem Abschnitt.

Zeigen Sie das Dialogfeld **Eigenschaften** für dieses Richtlinienobjekt an und öffnen Sie die Registerkarte **Richtlinien**. Wählen Sie dann in der Liste die Richtlinie aus, und klicken Sie auf **Anzeigen/Bearbeiten**, um das Dialogfeld **Eigenschaften der Benutzerkonto-Deprovisionierungsrichtlinie** anzuzeigen.

Die Registerkarte **Zu aktualisierende Eigenschaften** im Dialogfeld **Eigenschaften der Benutzerkonto-Deprovisionierungsrichtlinie** ähnelt der Seite **Zu aktualisierende Eigenschaften** des Assistenten, mit dem Sie das Richtlinienobjekt konfiguriert haben. Mit dieser Registerkarte können Sie wie folgt die Aktualisierungsregel für die Eigenschaft **Hinweise** hinzufügen:

1. Klicken Sie auf **Hinzufügen**, um das Dialogfeld **Objekteigenschaft wählen** anzuzeigen.
2. Aktivieren Sie das Kontrollkästchen neben der Eigenschaft **Hinweise** und klicken Sie dann auf **OK**.
3. Geben Sie im Dialogfeld **Wert hinzufügen** in das Feld **„Hinweise" muss sein** den Wert **Deprovisioniert** ein und klicken Sie dann auf **OK**.

Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften der Benutzerkonto-Deprovisionierungsrichtlinie** zu schließen.

Schritt 3: Anwenden des Richtlinienobjekts

Um das Richtlinienobjekt anzuwenden, können Sie im Dialogfeld **Eigenschaften** für dieses Richtlinienobjekt die Registerkarte **Bereich** verwenden:

1. Klicken Sie auf der Registerkarte **Bereich** auf die Schaltfläche **Bereich**, um das Fenster **ActiveRoles Serverrichtlinienbereich** für das zu verwaltende Richtlinienobjekt anzuzeigen.
2. Klicken Sie auf **Hinzufügen** und wählen Sie die Domäne, Organisationseinheit oder verwaltete Einheit aus, auf die Sie die Richtlinie anwenden möchten.

   *Sie können auch mit Hilfe der Schaltfläche **Entfernen** Elemente entfernen, auf die die Richtlinie nicht mehr angewendet werden soll.*
3. Klicken Sie auf **OK**, um das Fenster **ActiveRoles Serverrichtlinienbereich** zu schließen.
4. Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften** für das Richtlinienobjekt zu schließen.

Weitere Informationen über die Anwendung eines Richtlinienobjekts finden Sie unter „Anwenden von Richtlinienobjekten" und „Verwalten des Richtlinienbereichs" weiter oben in diesem Kapitel.

Entfernen der Gruppenmitgliedschaft

Richtlinien dieser Kategorie dienen zur Automatisierung des Entfernens von deprovisionierten Benutzerkonten. Eine Richtlinie kann so konfiguriert werden, dass sie Benutzerkonten aus allen Gruppen entfernt, dabei jedoch optional Ausnahmen macht. Einzelne Richtlinienregeln können auf Sicherheitsgruppen und auf E-Mail-fähige Gruppen vom Sicherheits- oder Verteilungstyp angewandt werden.

Funktionsweise dieser Richtlinie

Beim Verarbeiten einer Deprovisionsanforderung für einen Benutzer verwendet ActiveRoles Server diese Richtlinie, um zu bestimmen, welche Änderungen an Gruppenmitgliedschaften des Benutzerkontos vorgenommen werden sollen. Indem sie das Konto aus Sicherheitsgruppen entfernt, widerruft die Richtlinie Zugriffsrechte des Benutzers für Ressourcen. Indem sie das Konto aus E-Mail-fähigen Gruppen entfernt, verhindert die Richtlinie fehlerhafte Situationen, in denen E-Mail an das deprovisionierte Postfach gesendet wird.

Die Benutzer, für die die Bereitstellung zurückgenommen wurde, werden automatisch aus allen dynamischen Gruppen entfernt, unabhängig von den Einstellungen der Richtlinie „Entfernen der Gruppenmitgliedschaft".

Die Richtlinie „Entfernen der Gruppenmitgliedschaft" enthält separate Regeln für Sicherheitsgruppen und E-Mail-fähige Gruppen. Für jede Kategorie von Gruppen kann ActiveRoles Server anhand einer Regel eine der Aktionen ausführen, die in der folgenden Tabelle zusammengefasst sind.

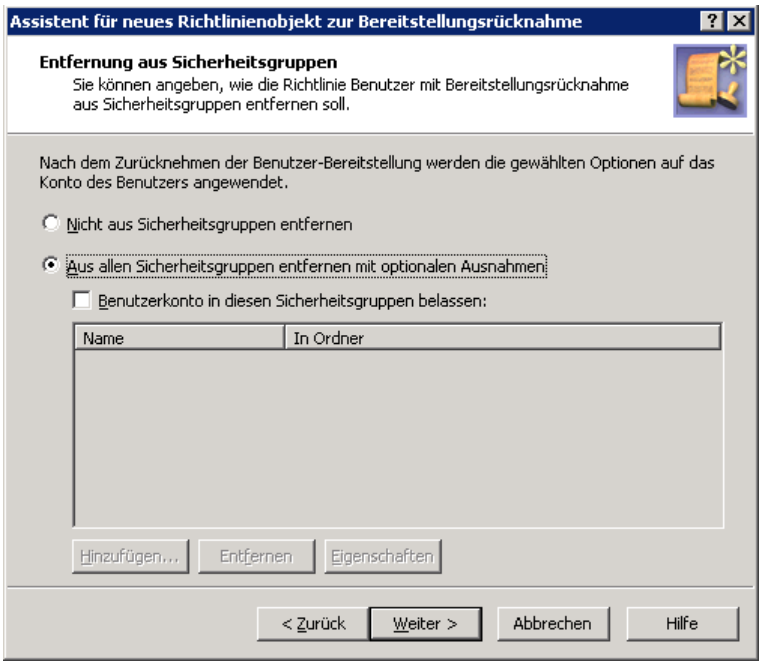
KATEGORIE	VORGANG	ERGEBNIS
Sicherheits-gruppen	Kein Entfernen aus Gruppen	Der Benutzer, für den die Bereitstellung zurückgenommen wurde, verbleibt in allen Sicherheitsgruppen, in denen zum Zeitpunkt der Zurücknahme eine Mitgliedschaft bestand, außer in den dynamischen Gruppen.
	Entfernen aus allen Gruppen	Der Benutzer, für den die Bereitstellung zurückgenommen wurde, wird aus allen Sicherheitsgruppen entfernt.
	Entfernen aus allen Gruppen außer den angegebenen	Der Benutzer, für den die Bereitstellung zurückgenommen wurde, wird aus den angegebenen Sicherheitsgruppen nicht entfernt, außer aus dynamischen Gruppen. Aus allen anderen Sicherheitsgruppen wird der Benutzer entfernt.
E-Mail-fähige Gruppen	Kein Entfernen aus Gruppen	Der Benutzer, für den die Bereitstellung zurückgenommen wurde, verbleibt in den Verteilergruppen und E-Mail-fähigen Gruppen, außer in den dynamischen Gruppen.
	Entfernen aus allen Gruppen	Der Benutzer, für den die Bereitstellung zurückgenommen wurde, wird aus allen Verteilergruppen und allen E-Mail-fähigen Sicherheitsgruppen entfernt.
	Entfernen aus allen Gruppen außer den angegebenen	Der Benutzer, für den die Bereitstellung zurückgenommen wurde, wird aus den angegebenen Verteilergruppen und E-Mail-fähigen Sicherheits-gruppen nicht entfernt, außer aus dynamischen Gruppen. Aus allen anderen Verteilergruppen und E-Mail-fähigen Sicherheitsgruppen wird der Benutzer entfernt.

Bei einem Konflikt in der Richtlinienimplementierung hat die Entfernungsaktion Vorrang. Beispielsweise wird mit einer Regel, die für das Entfernen des Benutzerkontos aus allen Sicherheitsgruppen konfiguriert ist, das Benutzerkonto auch dann aus allen Sicherheitsgruppen entfernt, wenn eine weitere Regel vorhanden ist, die angibt, dass ActiveRoles Server das Benutzerkonto aus E-Mail-fähigen Sicherheits-gruppen nicht entfernen soll.

Ein weiterer Konflikt kann auftreten, wenn eine Richtlinie dieser Kategorie versucht, einen Benutzer mit zurückgenommener Bereitstellung aus einer Gruppe zu entfernen, die als dynamische Gruppe von ActiveRoles Server konfiguriert ist (siehe das Kapitel „Dynamische Gruppen" weiter unten in diesem Dokument). Die Richtlinie für dynamische Gruppen erkennt, dass der Benutzer entfernt wurde, und kann den Benutzer wieder zur dynamischen Gruppe hinzufügen. Um eine solche Situation zu vermeiden, lässt ActiveRoles Server nicht zu, dass dynamische Gruppen deprovisionierte Benutzer enthalten. Nach der Deprovisionierung wird das Konto des Benutzers aus allen dynamischen Gruppen entfernt.

Konfigurieren der Richtlinie „Entfernen der Gruppenmitgliedschaft"

Um die Richtlinie „Entfernen der Gruppenmitgliedschaft" zu konfigurieren, wählen Sie **Entfernen der Gruppenmitgliedschaft** auf der Seite **Zu konfigurierende Richtlinie** im Assistenten „Neues Deprovisionsrichtlinienobjekt" oder im Assistenten „Deprovisionsrichtlinie hinzufügen" aus. Klicken Sie dann auf **Weiter**, damit die Seite **Entfernung aus Sicherheitsgruppen** angezeigt wird.


Assistent für neues Richtlinienobjekt zur Bereitstellungsrücknahme
Entfernung aus Sicherheitsgruppen
Sie können angeben, wie die Richtlinie Benutzer mit Bereitstellungsrücknahme aus Sicherheitsgruppen entfernen soll.
Nach dem Zurücknehmen der Benutzer-Bereitstellung werden die gewählten Optionen auf das Konto des Benutzers angewendet.
Nicht aus Sicherheitsgruppen entfernen
Aus allen Sicherheitsgruppen entfernen mit optionalen Ausnahmen
Benutzerkonto in diesen Sicherheitsgruppen belassen:
Name
In Ordner
Hinzufügen...
Entfernen
Eigenschaften
< Zurück
Weiter >
Abbrechen
Hilfe

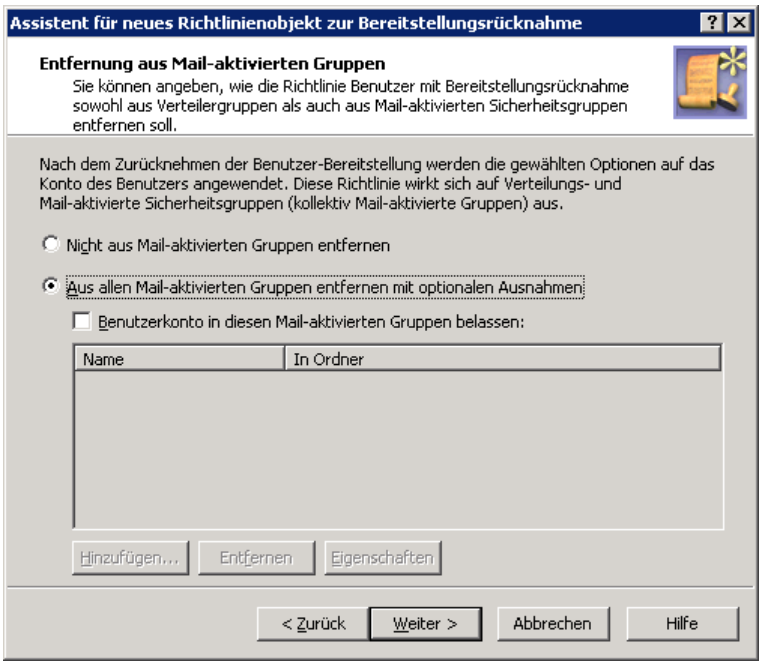
Auf dieser Seite können Sie eine Regel konfigurieren, die angibt, wie ein Benutzer mit zurückgenommener Bereitstellung aus Sicherheitsgruppen entfernt werden soll.

Wählen Sie eine der folgenden Optionen aus:

- Klicken Sie auf **Nicht aus Sicherheitsgruppen entfernen**, damit die Richtlinie keine Änderungen an der Sicherheitsgruppenmitgliedschaft des Benutzerkontos vornimmt.
- Klicken Sie auf **Aus allen Sicherheitsgruppen entfernen mit optionalen Ausnahmen**, damit die Richtlinie das Benutzerkonto aus allen Sicherheitsgruppen entfernt.

Mit der zweiten Option können Sie angeben, ob die Richtlinie das Objekt in bestimmten Sicherheitsgruppen belassen soll. Um eine Liste solcher Gruppen einzurichten, aktivieren Sie das Kontrollkästchen **Benutzerkonto in diesen Sicherheitsgruppen belassen**, klicken Sie dann auf die Schaltfläche **Hinzufügen**, und wählen Sie die Gruppen aus, die Sie in die Liste einschließen möchten.

Klicken Sie nach dem Konfigurieren der Regel für Sicherheitsgruppen auf **Weiter**, um die Seite **Entfernung aus Mail-aktivierten Gruppen** anzuzeigen.


Assistent für neues Richtlinienobjekt zur Bereitstellungsrücknahme
Entfernung aus Mail-aktivierten Gruppen
Sie können angeben, wie die Richtlinie Benutzer mit Bereitstellungsrücknahme sowohl aus Verteilergruppen als auch aus Mail-aktivierten Sicherheitsgruppen entfernen soll.
Nach dem Zurücknehmen der Benutzer-Bereitstellung werden die gewählten Optionen auf das Konto des Benutzers angewendet. Diese Richtlinie wirkt sich auf Verteilungs- und Mail-aktivierte Sicherheitsgruppen (kollektiv Mail-aktivierte Gruppen) aus.
Nicht aus Mail-aktivierten Gruppen entfernen
Aus allen Mail-aktivierten Gruppen entfernen mit optionalen Ausnahmen
Benutzerkonto in diesen Mail-aktivierten Gruppen belassen:
Name
In Ordner
Hinzufügen...
Entfernen
Eigenschaften
< Zurück
Weiter >
Abbrechen
Hilfe

Diese Seite ähnelt der vorigen. Sie ermöglicht das Konfigurieren einer Regel, anhand derer ein Benutzerkonto sowohl aus Verteilergruppen als auch aus E-Mail-fähigen Sicherheitsgruppen entfernt wird. Diese Gruppen werden zusammen als E-Mail-fähige Gruppen bezeichnet.

Wählen Sie eine der folgenden Optionen aus:

- Klicken Sie auf **Nicht aus Mail-aktivierten Gruppen entfernen**, damit die Richtlinie keine Änderungen an der Mitgliedschaft des Benutzerkontos in E-Mail-fähigen Gruppen vornimmt.
- Klicken Sie auf **Aus allen Mail-aktivierten Gruppen entfernen mit optionalen Ausnahmen**, damit die Richtlinie das Benutzerkonto aus allen E-Mail-fähigen Gruppen entfernt.

Mit der zweiten Option können Sie angeben, ob die Richtlinie das Objekt in bestimmten E-Mail-fähigen Gruppen belassen soll. Um eine Liste solcher Gruppen einzurichten, aktivieren Sie das Kontrollkästchen **Benutzerkonto in diesen Mail-aktivierten Gruppen belassen**, klicken Sie dann auf die Schaltfläche **Hinzufügen**, und wählen Sie die Gruppen aus, die Sie in die Liste einschließen möchten.

Klicken Sie nach dem Konfigurieren der Regel für E-Mail-fähige Gruppen auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schrittweise Anleitungen finden Sie unter **Anleitungen/Verwalten von Richtlinienobjekten/ Konfigurieren von Deprovisionsrichtlinienobjekten/Konfigurieren einer Richtlinie zum Entfernen von Gruppenmitgliedschaften** in der ActiveRoles Server-Hilfe.

Szenario: Entfernen von Benutzern mit zurückgenommener Bereitstellung aus allen Gruppen

Die in diesem Szenario beschriebenen Richtlinie entfernt die Benutzer mit zurückgenommener Bereitstellung aus allen Gruppen, also aus Sicherheits- und Verteilergruppen.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen und konfigurieren Sie das Richtlinienobjekt, das die entsprechende Richtlinie definiert.
2. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Bei der Deprovision für ein Benutzerkonto in dem Container, den Sie in Schritt 2 ausgewählt haben, entfernt ActiveRoles Server folglich das Benutzerkonto aus allen Gruppen.

In den folgenden beiden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen und Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt mit dem Assistenten „Neues Deprovisionsrichtlinienobjekt" erstellen und konfigurieren. Weitere Informationen über den Assistenten finden Sie unter „Erstellen eines Richtlinienobjekts" im Abschnitt „Verwaltungsaufgaben für Richtlinienobjekte" weiter oben in diesem Kapitel.

Klicken Sie zum Konfigurieren der Richtlinie auf der Seite **Richtlinientyp auswählen** des Assistenten auf **Entfernen der Gruppenmitgliedschaft**. Klicken Sie dann auf **Weiter**, und führen Sie die folgenden Schritte aus:

1. Auf der Seite **Entfernung aus Sicherheitsgruppen**:
   a) Klicken Sie auf **Aus allen Sicherheitsgruppen entfernen mit optionalen Ausnahmen**.
   b) Stellen Sie sicher, dass das Kontrollkästchen **Benutzerkonto in diesen Sicherheitsgruppen belassen** deaktiviert ist.
   c) Klicken Sie auf **Weiter**.
2. Auf der Seite **Entfernung aus Mail-aktivierten Gruppen**:
   a) Klicken Sie auf **Aus allen Mail-aktivierten Gruppen entfernen mit optionalen Ausnahmen**.
   b) Stellen Sie sicher, dass das Kontrollkästchen **Benutzerkonto in diesen Mail-aktivierten Gruppen belassen** deaktiviert ist.
   c) Klicken Sie auf **Weiter**.
3. Klicken Sie auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schritt 2: Anwenden des Richtlinienobjekts

Sie können das Richtlinienobjekt mit Hilfe der Seite **Richtlinie erzwingen** im Assistenten „Neues Deprovisionsrichtlinienobjekt" anwenden oder Sie können den Assistenten erst abschließen und dann den Befehl **Richtlinie erzwingen** für die Domäne, die Organisationseinheit oder die verwaltete Einheit verwenden, auf die Sie die Richtlinie anwenden möchten.

Weitere Informationen über die Anwendung eines Richtlinienobjekts finden Sie unter „Anwenden von Richtlinienobjekten" und „Verwalten des Richtlinienbereichs" weiter oben in diesem Kapitel.

Deprovisionierung des Exchange-Postfachs

Richtlinien dieser Kategorie dienen zum Automatisieren der folgenden Aufgaben, mit denen für Benutzer mit zurückgenommener Bereitstellung Microsoft Exchange-Ressourcen deprovisioniert werden:

- Verbergen von Benutzern mit zurückgenommener Bereitstellung in Adressenlisten
- Verhindern, dass Unzustellbarkeitsberichte gesendet werden
- Gewähren von Lesezugriff für ausgewählte Personen auf deprovisionierte Postfächer
- Umleiten von E-Mails, die an Benutzer mit zurückgenommener Bereitstellung gerichtet sind

Beim Konfigurieren einer Richtlinie dieser Kategorie geben Sie an, wie ActiveRoles Server das Konto und das Postfach des Benutzers ändern soll, wenn für den Benutzer eine Deprovisionsanforderung vorliegt. Damit wird bezweckt, dass weniger E-Mails an diesen Benutzer gesendet werden und dass ausgewählte Personen zum Überwachen solcher E-Mails autorisiert werden.

Funktionsweise dieser Richtlinie

Beim Verarbeiten einer Deprovisionsanforderung für einen Benutzer verwendet ActiveRoles Server diese Richtlinie, um die Optionen für die Deprovisionierung von Exchange-Postfach zu bestimmen, und aktualisiert das Konto sowie das Postfach des Benutzers dann entsprechend.

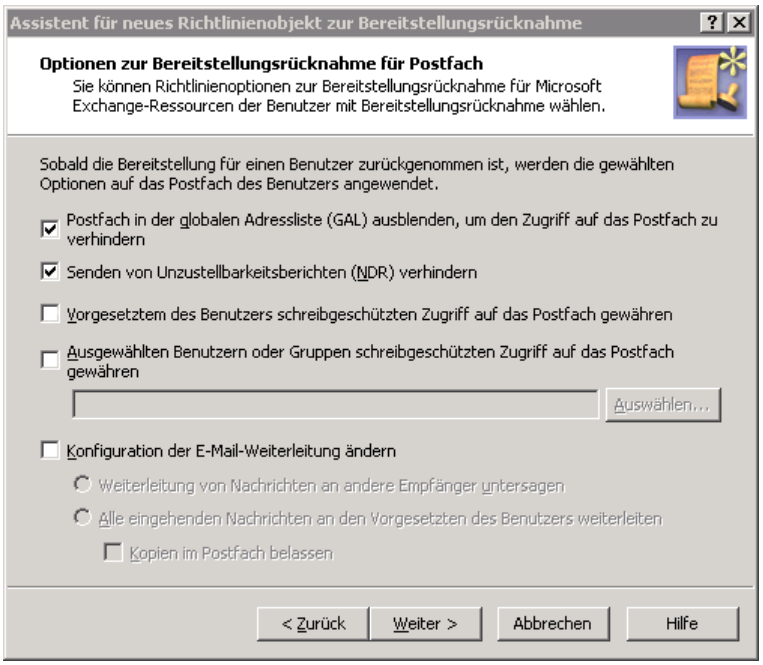
Die verfügbaren Optionen für die Postfachdeprovisionierung werden in der folgenden Tabelle zusammengefasst. Für jede Option wird in der Tabelle die Auswirkung der Richtlinie auf das Benutzerpostfach umrissen.

OPTION	AUSWIRKUNG DER RICHTLINIE
Ausblenden des Postfachs aus der globalen Adressliste	Verhindert, dass der Benutzer mit zurückgenommener Bereitstellung in der Exchange-Adressenliste der Organisation angezeigt wird. Wenn Sie diese Option aktivieren, wird der Benutzer in allen Adressenlisten verborgen. Außer wenn der Lesezugriff auf das Postfach einem bestimmten Benutzer oder einer bestimmten Gruppe in Active Directory explizit gewährt wurde, führt diese Option dazu, dass auf das Postfach nicht mehr zugegriffen werden kann. Sie können sich nicht als der Postfachbenutzer bei Exchange Server anmelden und nicht anderweitig auf das verborgene Postfach zugreifen.
Verhindern, dass Unzustellbarkeitsberichte gesendet werden	Verhindert, dass Unzustellbarkeitsberichte generiert werden, wenn E-Mails an das deprovisionierte Postfach gesendet werden. (Bei einem Unzustellbarkeits-bericht handelt es sich um die Benachrichtigung, dass eine Nachricht nicht an den Empfänger übermittelt wurde).
Vorgesetztem des Benutzers schreibgeschützten Zugriff auf das Postfach gewähren	Ermöglicht es der Person, die als Vorgesetzter des Benutzers mit zurückgenommener Bereitstellung bezeichnet ist, E-Mails im Postfach dieses Benutzers zu lesen. Der Vorgesetzte wird anhand des Attributs **Verwalter** des deprovisionierten Benutzerkontos in Active Directory bestimmt.
Ausgewählten Benutzern oder Gruppen schreib-geschützten Zugriff auf das Postfach gewähren	Ermöglicht es den angegebenen Benutzern oder Gruppen, E-Mails im Postfach dieses Benutzers zu lesen.
Weiterleiten von Nachrichten verbieten	Für diesen Benutzer bestimmte E-Mails werden nicht an einen alternativen Empfänger weitergeleitet.

OPTION	AUSWIRKUNG DER RICHTLINIE
Weiterleiten aller eingehenden Nachrichten an den Vorgesetzten des Benutzers	Für diesen Benutzer bestimmte E-Mails werden an den Vorgesetzten des Benutzers weitergeleitet. Der Vorgesetzte wird anhand des Attributs **Verwalter** des deprovisionierten Benutzerkontos in Active Directory bestimmt.
Kopien im Postfach belassen	Für diesen Benutzer bestimmte E-Mails werden an des Postfach das Benutzers und des Vorgesetzten übermittelt. Wenn Sie diese Option nicht aktivieren, werden solche E-Mails nur an das Postfach des Vorgesetzten übermittelt.

Konfigurieren der Richtlinie „Deprovisionierung des Exchange-Postfachs“

Um die Richtlinie „Deprovisionierung des Exchange-Postfachs“ zu konfigurieren, wählen Sie **Deprovisionierung des Exchange-Postfachs** auf der Seite **Zu konfigurierende Richtlinie** im Assistenten „Neues Deprovisionsrichtlinienobjekt“ oder im Assistenten „Deprovisionsrichtlinie hinzufügen“ aus. Klicken Sie dann auf **Weiter**, damit die Seite **Optionen zur Bereitstellungsrücknahme für Postfach** angezeigt wird.


Assistent für neues Richtlinienobjekt zur Bereitstellungsrücknahme
Optionen zur Bereitstellungsrücknahme für Postfach
Sie können Richtlinienoptionen zur Bereitstellungsrücknahme für Microsoft Exchange-Ressourcen der Benutzer mit Bereitstellungsrücknahme wählen.
Sobald die Bereitstellung für einen Benutzer zurückgenommen ist, werden die gewählten Optionen auf das Postfach des Benutzers angewendet.
Postfach in der globalen Adressliste (GAL) ausblenden, um den Zugriff auf das Postfach zu verhindern
Senden von Unzustellbarkeitsberichten (NDR) verhindern
Vorgesetztem des Benutzers schreibgeschützten Zugriff auf das Postfach gewähren
Ausgewählten Benutzern oder Gruppen schreibgeschützten Zugriff auf das Postfach gewähren
Auswählen...
Konfiguration der E-Mail-Weiterleitung ändern
Weiterleitung von Nachrichten an andere Empfänger untersagen
Alle eingehenden Nachrichten an den Vorgesetzten des Benutzers weiterleiten
Kopien im Postfach belassen
< Zurück
Weiter >
Abbrechen
Hilfe

Auf dieser Seite können Sie die Optionen für die Deprovisionierung von Exchange-Postfach für den Stammordner auswählen, die ActiveRoles Server bei der Deprovision für einen Benutzer anwenden soll. Die Namen der ersten vier Optionen sind selbsterklärend (siehe auch Tabelle oben):

- Postfach in der globalen Adressliste (GAL) ausblenden, um den Zugriff auf das Postfach zu verhindern
- Verhindern, dass Unzustellbarkeitsberichte gesendet werden
- Verwalter des Benutzers Vollzugriff auf das Postfach gewähren
- Ausgewählten Benutzern oder Gruppen Vollzugriff auf das Postfach gewähren

Aktivieren Sie die Kontrollkästchen neben den Optionen, die angewendet werden sollen. Für die vierte Option müssen Sie auf die Schaltfläche **Auswählen** klicken, um Benutzer oder Gruppen auszuwählen. Die ausgewählten Benutzer und Gruppen werden autorisiert, auf die Postfächer der Benutzer mit zurückgenommener Bereitstellung zuzugreifen.

Sie können die Richtlinie auch so konfigurieren, dass sie die Weiterleitungsadresse für die deprovisionierten Benutzer ändert. Wenn Sie das Kontrollkästchen **Konfiguration der E-Mail-Weiterleitung ändern** aktivieren, legt die Richtlinie die Weiterleitungsadresse auf einen der folgenden Werte fest:

- **Kein** Um anzugeben, dass E-Mail-Nachrichten an einen Benutzer mit zurückgenommener Bereitstellung nicht weitergeleitet werden sollen, klicken Sie auf **Weiterleitung von Nachrichten an andere Empfänger untersagen**.
- **Verwalter des Benutzers** Um anzugeben, dass E-Mail-Nachrichten an einen Benutzer mit zurückgenommener Bereitstellung an den Vorgesetzten des Benutzers weitergeleitet werden sollen, klicken Sie auf **Alle eingehenden Nachrichten an den Vorgesetzten des Benutzers weiterleiten**.

Mit der zweiten Option können Sie angeben, ob E-Mail-Nachrichten an den Benutzer mit zurückgenommener Bereitstellung an das Postfach des Benutzers übermittelt werden sollen:

- Wenn Sie das Kontrollkästchen **Kopien im Postfach belassen** aktivieren, werden die Nachrichten an des Postfach des Benutzers und des Vorgesetzten übermittelt.
- Wenn Sie das Kontrollkästchen **Kopien im Postfach belassen** deaktivieren, werden die Nachrichten nur an das Postfach des Vorgesetzten übermittelt.

Klicken Sie nach Abschluss des Vorgangs auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schrittweise Anleitungen finden Sie unter **Anleitungen/Verwalten von Richtlinienobjekten/ Konfigurieren von Deprovisionsrichtlinienobjekten/Konfigurieren einer Richtlinie zur Deprovisionierung von Exchange-Postfächern** in der ActiveRoles Server-Hilfe.

Szenario: Ausblenden eines Postfachs und Weiterleiten der E-Mails an den Vorgesetzten

Die in diesem Szenario beschriebene Richtlinie führt während der Deprovision für einen Benutzer die folgenden Funktionen aus:

- Blendet den Benutzer mit zurückgenommener Bereitstellung in den Exchange-Adressenlisten der Organisation aus.
- Konfiguriert die E-Mail-Weiterleitung so, dass E-Mail-Nachrichten an den Benutzer mit zurückgenommener Bereitstellung an den Vorgesetzten des Benutzers gesendet werden, nicht jedoch an das Postfach des Benutzers.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen und konfigurieren Sie das Richtlinienobjekt, das die entsprechende Richtlinie definiert.
2. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Bei der Deprovision für ein Benutzerkonto in dem Container, den Sie in Schritt 2 ausgewählt haben, blendet ActiveRoles Server folglich den Benutzer in den Exchange-Adressenlisten aus und konfiguriert die Weiterleitungsadresse für den Benutzer gemäß der Vorschrift in dieser Richtlinie.

In den folgenden beiden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen und Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt mit dem Assistenten „Neues Deprovisionsrichtlinienobjekt" erstellen und konfigurieren. Weitere Informationen über den Assistenten finden Sie unter „Erstellen eines Richtlinienobjekts" im Abschnitt „Verwaltungsaufgaben für Richtlinienobjekte" weiter oben in diesem Kapitel.

Klicken Sie zum Konfigurieren der Richtlinie auf der Seite **Richtlinientyp auswählen** des Assistenten auf **Deprovisionierung des Exchange-Postfachs**. Klicken Sie dann auf **Weiter**.

Aktivieren Sie auf der Seite **Optionen zur Bereitstellungsrücknahme für Postfach** die folgenden Kontrollkästchen:

- **Postfach in der globalen Adressliste (GAL) ausblenden, um den Zugriff auf das Postfach zu verhindern**
- **Konfiguration der E-Mail-Weiterleitung ändern**

Stellen sie sicher, dass keine anderen Kontrollkästchen auf der Seite aktiviert sind. Klicken Sie dann auf **Alle eingehenden Nachrichten an den Vorgesetzten des Benutzers weiterleiten**, und deaktivieren Sie das Kontrollkästchen **Kopien im Postfach belassen**.

Klicken Sie nach Abschluss des Vorgangs auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schritt 2: Anwenden des Richtlinienobjekts

Sie können das Richtlinienobjekt mit Hilfe der Seite **Richtlinie erzwingen** im Assistenten „Neues Deprovisionsrichtlinienobjekt" anwenden oder Sie können den Assistenten erst abschließen und dann den Befehl **Richtlinie erzwingen** für die Domäne, die Organisationseinheit oder die verwaltete Einheit verwenden, auf die Sie die Richtlinie anwenden möchten.

Weitere Informationen über die Anwendung eines Richtlinienobjekts finden Sie unter „Anwenden von Richtlinienobjekten" und „Verwalten des Richtlinienbereichs" weiter oben in diesem Kapitel.

Stammordner-Deprovisionierung

Richtlinien dieser Kategorie dienen zum Automatisieren der folgenden Aufgaben, mit denen für Benutzer mit zurückgenommener Bereitstellung Stammordner deprovisioniert werden:

- Aufheben des Zugriffs auf Stammordner für deprovisionierte Benutzerkonten
- Gewähren von Lesezugriff für ausgewählte Personen auf deprovisionierte Stammordner
- Ändern des Besitzers für deprovisionierte Stammordner
- Löschen deprovisionierter Stammordner

Beim Konfigurieren einer Richtlinie dieser Kategorie geben Sie an, wie ActiveRoles Server bei einer Deprovisionsanforderung für einen Benutzer die Sicherheit für den Stammordner des Benutzers ändern soll und ob ActiveRoles Server beim Löschen eines Benutzerkontos auch Stammordner löschen soll. Damit wird bezweckt, dass Benutzer mit zurückgenommener Bereitstellung am Zugreifen auf ihre Stammordner gehindert werden und dass ausgewählte Personen zum Zugreifen auf solche Stammordner autorisiert werden.

Funktionsweise dieser Richtlinie

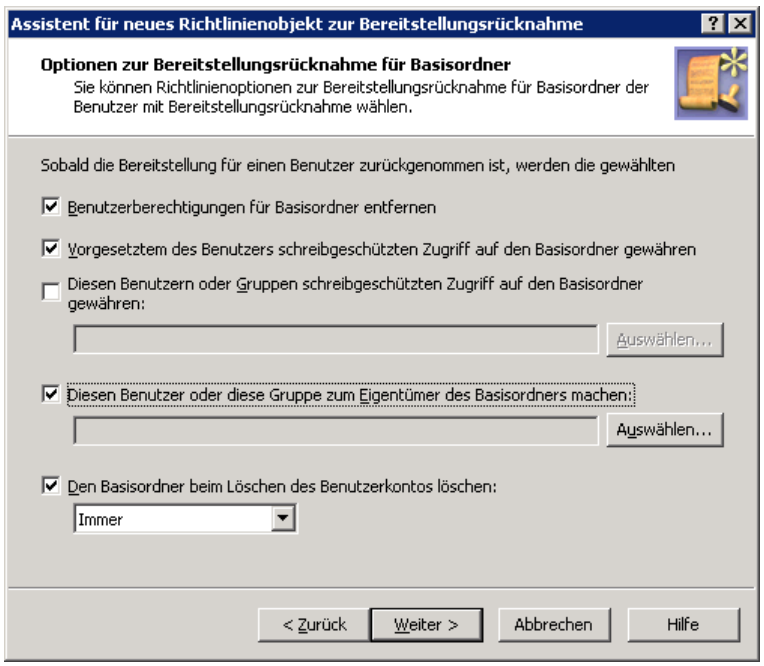
Beim Verarbeiten einer Deprovisionsanforderung für einen Benutzer verwendet ActiveRoles Server diese Richtlinie, um die Optionen für die Deprovisionierung des Stammordners zu bestimmen, und aktualisiert die Stammordnerkonfiguration des Benutzers dann entsprechend.

Die verfügbaren Optionen für die Stammordner-Deprovisionierung werden in der folgenden Tabelle zusammengefasst. Für jede Option wird in der Tabelle die Auswirkung der Richtlinie auf den Benutzerstammordner umrissen.

OPTION	AUSWIRKUNG DER RICHTLINIE
Entfernen der Berechtigungen des Benutzers für den Stammordner	Ändert die Sicherheit für den Stammordner so, dass der Benutzer nicht mehr darauf zugreifen kann.
Vorgesetztem des Benutzers schreibgeschützten Zugriff auf den Stammordner gewähren	Ermöglicht es der Person, die als Vorgesetzter des Benutzers mit zurückgenommener Bereitstellung bezeichnet ist, Daten im Stammordner dieses Benutzers anzuzeigen und abzurufen. Der Vorgesetzte wird anhand des Attributs **Verwalter** des deprovisionierten Benutzerkontos in Active Directory bestimmt.
Ausgewählten Benutzern oder Gruppen schreibgeschützten Zugriff auf den Stammordner gewähren	Ermöglicht es den angegebenen Benutzern oder Gruppen, Daten im Stammordner dieses Benutzers anzuzeigen und abzurufen.
Den ausgewählten Benutzer oder die ausgewählte Gruppe zum Besitzer des Stammordners machen	Legt den ausgewählten Benutzer oder die ausgewählte Gruppe als Besitzer des Stammordners dieses Benutzers fest. Der Besitzer ist dazu autorisiert, die Festlegung von Berechtigung für den Ordner zu steuern, und kann anderen Berechtigungen erteilen.
Den Stammordner beim Löschen des Benutzerkontos löschen	Analysiert beim Löschen eines Benutzerkontos, ob der Stammordner des Benutzers leer ist, und löscht den Stammordner dann abhängig von der Richtlinienkonfiguration oder behält ihn bei. Eine Richtlinie kann so konfiguriert werden, dass sie nur leere Ordner löscht. Es besteht auch die Option, leere und nicht leere Ordner zu löschen.

Konfigurieren der Richtlinie „Stammordner-Deprovisionierung“

Um die Richtlinie „Stammordner-Deprovisionierung“ zu konfigurieren, wählen Sie **Stammordner-Deprovisionierung** auf der Seite **Zu konfigurierende Richtlinie** im Assistenten „Neues Deprovisionsrichtlinienobjekt“ oder im Assistenten „Deprovisionsrichtlinie hinzufügen“ aus. Klicken Sie dann auf **Weiter**, damit die Seite **Optionen zur Bereitstellungsrücknahme für Basisordner** angezeigt wird.


Assistent für neues Richtlinienobjekt zur Bereitstellungsrücknahme
Optionen zur Bereitstellungsrücknahme für Basisordner
Sie können Richtlinienoptionen zur Bereitstellungsrücknahme für Basisordner der Benutzer mit Bereitstellungsrücknahme wählen.
Sobald die Bereitstellung für einen Benutzer zurückgenommen ist, werden die gewählten
Benutzerberechtigungen für Basisordner entfernen
Vorgesetztem des Benutzers schreibgeschützten Zugriff auf den Basisordner gewähren
Diesen Benutzern oder Gruppen schreibgeschützten Zugriff auf den Basisordner gewähren:
Auswählen...
Diesen Benutzer oder diese Gruppe zum Eigentümer des Basisordners machen:
Auswählen...
Den Basisordner beim Löschen des Benutzerkontos löschen:
Immer
< Zurück
Weiter >
Abbrechen
Hilfe

Auf dieser Seite können Sie die Deprovisionierungsoptionen für den Stammordner auswählen, die ActiveRoles Server bei der Deprovision für einen Benutzer anwenden soll.

Die Namen der ersten vier Optionen sind selbsterklärend. Sie beziehen sich auf die Richtlinienoptionen, die in der Tabelle oben zusammengefasst sind:

- Entfernen der Berechtigungen des Benutzers für den Stammordner
- Vorgesetztem des Benutzers schreibgeschützten Zugriff auf den Stammordner gewähren
- Diesen Benutzern oder Gruppen schreibgeschützten Zugriff auf den Stammordner gewähren
- Diesen Benutzer oder diese Gruppe zum Besitzer des Stammordners machen

Aktivieren Sie die Kontrollkästchen neben den Optionen, die angewendet werden sollen.

Für die dritte Option müssen Sie auf die Schaltfläche **Auswählen** klicken, um Benutzer oder Gruppen auszuwählen. Die ausgewählten Benutzer oder Gruppen werden autorisiert, Daten in den Stammordnern der Benutzer mit zurückgenommener Bereitstellung anzuzeigen und abzurufen.

Für die vierte Option müssen Sie auf die Schaltfläche **Auswählen** klicken, um einen Benutzer oder eine Gruppe auszuwählen. Der ausgewählte Benutzer oder die ausgewählte Gruppe wird autorisiert, Berechtigungen für die Stammordner der Benutzer mit zurückgenommener Bereitstellung zu steuern.

Sie können die Richtlinie auch so konfigurieren, dass sie Stammordner löscht. Wenn Sie das Kontrollkästchen **Den Stammordner beim Löschen des Benutzerkontos löschen** aktivieren, löscht ActiveRoles Server aufgrund dieser Richtlinie den Stammordner, sobald das ihm zugeordnete Benutzerkonto gelöscht wird. Sie können dieses Verhalten genauer steuern, indem Sie in der Liste unter dem Kontrollkästchen eine der folgenden Optionen auswählen:

- **Wenn Stammordner leer ist** Verhindert, dass ActiveRoles Server nicht leere Stammordner löscht. Wenn ein Stammordner beliebige Daten enthält, löscht die Richtlinie ihn nicht.
- **Immer** Ermöglicht ActiveRoles Server das Löschen leerer und nicht leerer Stammordner. Unabhängig davon, ob ein Stammordner Daten enthält, löscht die Richtlinie ihn bei der Löschung des Benutzerkontos.

Klicken Sie nach Abschluss des Vorgangs auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schrittweise Anleitungen finden Sie unter **Anleitungen/Verwalten von Richtlinienobjekten/ Konfigurieren von Deprovisionsrichtlinienobjekten/Konfigurieren einer Stammordner-Deprovisionierungsrichtlinie** in der ActiveRoles Server-Hilfe.

Szenario: Entfernen des Zugriffs auf einen Stammordner

Die in diesem Szenario beschriebene Richtlinie führt während der Deprovision für einen Benutzer die folgenden Funktionen aus:

- Entfernen aller Berechtigungen des Benutzers für den eigenen Stammordner.
- Legt die Administratorengruppe als Besitzer deprovisionierter Stammordner fest.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen und konfigurieren Sie das Richtlinienobjekt, das die entsprechende Richtlinie definiert.
2. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Bei der Deprovision für ein Benutzerkonto in dem Container, den Sie in Schritt 2 ausgewählt haben, ändert ActiveRoles Server folglich die Sicherheit für den Stammordner des Benutzers, wie von dieser Richtlinie vorgeschrieben.

In den folgenden beiden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen und Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt mit dem Assistenten „Neues Deprovisionsrichtlinienobjekt" erstellen und konfigurieren. Weitere Informationen über den Assistenten finden Sie unter „Erstellen eines Richtlinienobjekts" im Abschnitt „Verwaltungsaufgaben für Richtlinienobjekte" weiter oben in diesem Kapitel.

Klicken Sie zum Konfigurieren der Richtlinie auf der Seite **Richtlinientyp auswählen** des Assistenten auf **Stammordner-Deprovisionierung**. Klicken Sie dann auf **Weiter**.

Aktivieren Sie auf der Seite **Optionen zur Bereitstellungsrücknahme für Basisordner** die folgenden Kontrollkästchen:

- **Entfernen der Berechtigungen des Benutzers für den Stammordner**
- **Vorgesetztem des Benutzers schreibgeschützten Zugriff auf den Stammordner gewähren**

Stellen sie sicher, dass keine anderen Kontrollkästchen auf der Seite aktiviert sind. Klicken Sie dann auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schritt 2: Anwenden des Richtlinienobjekts

Sie können das Richtlinienobjekt mit Hilfe der Seite **Richtlinie erzwingen** im Assistenten „Neues Deprovisionsrichtlinienobjekt" anwenden oder Sie können den Assistenten erst abschließen und dann den Befehl **Richtlinie erzwingen** für die Domäne, die Organisationseinheit oder die verwaltete Einheit verwenden, auf die Sie die Richtlinie anwenden möchten.

Weitere Informationen über die Anwendung eines Richtlinienobjekts finden Sie unter „Anwenden von Richtlinienobjekten" und „Verwalten des Richtlinienbereichs" weiter oben in diesem Kapitel.

Benutzerkonto-Verschiebung

Richtlinien dieser Kategorie dienen zum Automatisieren der Verschiebung von deprovisionierten Benutzerkonten in angegebene Organisationseinheiten. So werden solche Konten der Steuerung der Administratoren entzogen, die die Organisationseinheiten verwalten, in denen sich diese Konten ursprünglich befanden. Eine Richtlinie dieser Kategorie kann auch so konfiguriert werden, dass sie deprovisionierte Benutzerkonten nicht verschiebt.

Funktionsweise dieser Richtlinie

Beim Verarbeiten einer Deprovisionsanforderung für einen Benutzer verwendet ActiveRoles Server diese Richtlinie, um zu bestimmen, ob das deprovisionierte Benutzerkonto in eine andere Organisationseinheit verschoben werden soll.

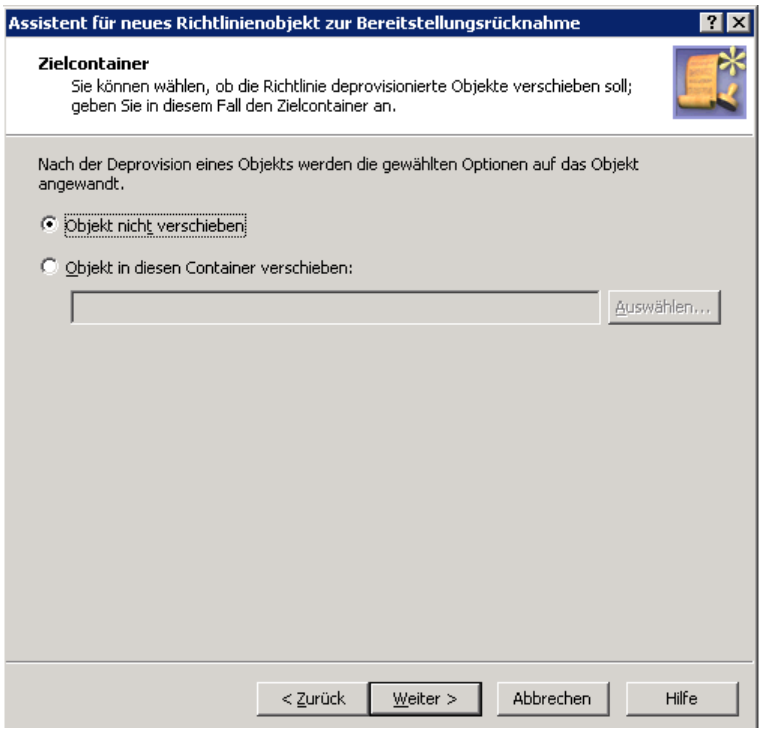
Eine für das Verschieben von Benutzerkonten konfigurierte Richtlinie gibt auch das Ziel an, also die Organisationseinheit, in die ActiveRoles Server deprovisionierte Benutzerkonten verschiebt.

Es kann auch eine Richtlinie konfiguriert werden, die Benutzerkonten nicht verschiebt. Wenn eine solche Richtlinie auf einer bestimmten Ebene der Verzeichnishierarchie angewendet wird, setzt sie ggf. alle anderen Richtlinien diese Kategorie außer Kraft, die auf einer höheren Ebene der Verzeichnishierarchie angewendet werden.

Das folgende Beispiel verdeutlicht dieses Verhalten. Nehmen Sie an, Sie konfigurieren eine Richtlinie für das Verschieben von Konten und wenden sie auf einen bestimmten übergeordneten Container an. Im Allgemeinen wird die Richtlinie vom übergeordneten Container an untergeordnete Container übergeben. Sie wird also auf alle untergeordneten Container des jeweiligen übergeordneten Containers angewendet, und ActiveRoles Server verschiebt folglich deprovisionierte Benutzerkonten aus allen diesen Containern. Wenn Sie jedoch eine andere Richtlinie konfigurieren, mit der Konten nicht verschoben werden, und diese neue Richtlinie auf einen untergeordneten Container anwenden, setzt die Richtlinie des untergeordneten Containers die vom übergeordneten Container geerbte Richtlinie außer Kraft. ActiveRoles Server verschiebt dann keine deprovisionierten Benutzerkonten aus diesem untergeordneten Container oder den Containern darunter.

Konfigurieren der Richtlinie „Benutzerkonto-Verschiebung“

Um die Richtlinie „Benutzerkonto-Verschiebung“ zu konfigurieren, wählen Sie **Benutzerkonto-Verschiebung** auf der Seite **Zu konfigurierende Richtlinie** im Assistenten „Neues Deprovisionsrichtlinienobjekt“ oder im Assistenten „Deprovisionsrichtlinie hinzufügen“ aus. Klicken Sie dann auf **Weiter**, damit die Seite **Zielcontainer** angezeigt wird.


Assistent für neues Richtlinienobjekt zur Bereitstellungsrücknahme
Zielcontainer
Sie können wählen, ob die Richtlinie deprovisionierte Objekte verschieben soll; geben Sie in diesem Fall den Zielcontainer an.
Nach der Deprovision eines Objekts werden die gewählten Optionen auf das Objekt angewandt.
Objekt nicht verschieben
Objekt in diesen Container verschieben:
Auswählen...
< Zurück
Weiter >
Abbrechen
Hilfe

Auf dieser Seite können Sie auswählen, ob die Richtlinie deprovisionierte Benutzerkonten verschieben soll, und Sie können den Zielcontainer für den Verschiebungsvorgang auswählen.

Wählen Sie zunächst eine der folgenden Optionen aus:

- Klicken Sie auf **Objekt nicht verschieben**, damit die Richtlinie deprovisionierte Benutzerkonten an ihren ursprünglichen Orten belässt. Mit dieser Option verbleibt jedes deprovisionierte Benutzerkonto in der Organisationseinheit, in der es sich bei der Rücknahme der Bereitstellung befand.
- Klicken Sie auf **Objekt in diesen Container verschieben**, damit die Richtlinie deprovisionierte Benutzerkonten in einen bestimmten Container verschiebt. Mit dieser Option wird jedes deprovisionierte Benutzerkonto von seinem ursprünglichen Ort in eine angegebene Organisationseinheit verschoben.

Für die zweite Option müssen Sie die Organisationseinheit angeben, in die die Richtlinie deprovisionierte Benutzerkonten verschieben soll. Klicken Sie auf die Schaltfläche **Auswählen** und wählen Sie dann die gewünschte Organisationseinheit aus.

Klicken Sie nach Abschluss des Vorgangs auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schrittweise Anleitungen finden Sie unter **Anleitungen/Verwalten von Richtlinienobjekten/ Konfigurieren von Deprovisionsrichtlinienobjekten/Konfigurieren einer Richtlinie zum Verschieben von Benutzerkonten** in der ActiveRoles Server-Hilfe.

Szenario: Organisationseinheit zum Ablegen deprovisionierter Benutzerkonten

In diesem Szenario wird das Konfigurieren einer Richtlinie beschrieben, die dazu führt, dass eine bestimmte Organisationseinheit alle deprovisionierten Benutzerkonten enthält.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen und konfigurieren Sie das Richtlinienobjekt, das die entsprechende Richtlinie definiert.
2. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Nach der Deprovision für ein Benutzerkonto in dem Container, den Sie in Schritt 2 ausgewählt haben, verschiebt ActiveRoles Server folglich dieses Konto automatisch in die von der Richtlinienkonfiguration bestimmte Organisationseinheit. In den folgenden beiden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen und Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt mit dem Assistenten „Neues Deprovisionsrichtlinienobjekt" erstellen und konfigurieren. Weitere Informationen über den Assistenten finden Sie unter „Erstellen eines Richtlinienobjekts" im Abschnitt „Verwaltungsaufgaben für Richtlinienobjekte" weiter oben in diesem Kapitel.

Klicken Sie zum Konfigurieren der Richtlinie auf der Seite **Richtlinientyp auswählen** des Assistenten auf **Benutzerkonto-Verschiebung**. Klicken Sie dann auf **Weiter**.

Klicken Sie auf der Seite **Zielcontainer** auf **Objekt in diesen Container verschieben**. Klicken Sie dann auf die Schaltfläche **Auswählen**, um das Dialogfeld **Container suchen** anzuzeigen. Suchen Sie die Organisationseinheit, in die die Richtlinie deprovisionierte Benutzerkonten verschieben soll, und wählen Sie sie aus. Klicken Sie dann auf **OK**.

Klicken Sie nach Abschluss des Vorgangs auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schritt 2: Anwenden des Richtlinienobjekts

Sie können das Richtlinienobjekt mit Hilfe der Seite **Richtlinie erzwingen** im Assistenten „Neues Deprovisionsrichtlinienobjekt" anwenden oder Sie können den Assistenten erst abschließen und dann den Befehl **Richtlinie erzwingen** für die Domäne, die Organisationseinheit oder die verwaltete Einheit verwenden, auf die Sie die Richtlinie anwenden möchten.

Weitere Informationen über die Anwendung eines Richtlinienobjekts finden Sie unter „Anwenden von Richtlinienobjekten" und „Verwalten des Richtlinienbereichs" weiter oben in diesem Kapitel.

Permanentes Löschen von Benutzerkonten

Richtlinien dieser Kategorie dienen zum Automatisieren der Löschung von deprovisionierten Benutzerkonten. Deprovisionierte Benutzerkonten werden für einen angegebenen Zeitraum beibehalten, bevor sie dauerhaft gelöscht werden. Eine Richtlinie dieser Kategorie kann auch so konfiguriert werden, dass sie deprovisionierte Konten nicht löscht.

Funktionsweise dieser Richtlinie

Beim Verarbeiten einer Deprovisionsanforderung für einen Benutzer verwendet ActiveRoles Server diese Richtlinie, um zu bestimmen, ob für das deprovisionierte Benutzerkonto die Löschung geplant werden soll. Ein Benutzerkonto, für das die Löschung geplant ist, wird nach einem bestimmten Zeitraum dauerhaft gelöscht. Dieser wird als *Wartezeitraum* bezeichnet.

Eine Richtlinie, die zum Löschen von Benutzerkonten konfiguriert ist, gibt an, für wie viele Tage deprovisionierte Benutzerkonten beibehalten werden sollen. Mit einer solchen Richtlinie löscht ActiveRoles Server ein Benutzerkonto nach der angegebenen Anzahl von Tagen seit der Deprovision für den Benutzer dauerhaft.

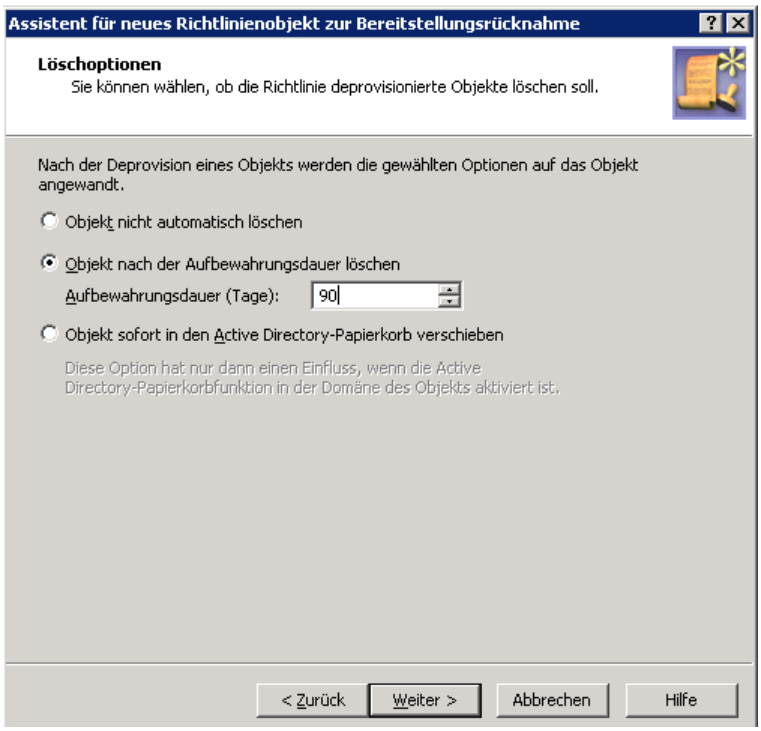
Es kann auch eine Richtlinie konfiguriert werden, die Benutzerkonten nicht löscht. Wenn eine solche Richtlinie auf einer bestimmten Ebene der Verzeichnishierarchie angewendet wird, setzt sie ggf. alle anderen Richtlinien diese Kategorie außer Kraft, die auf einer höheren Ebene der Verzeichnishierarchie angewendet werden.

Das folgende Beispiel verdeutlicht dieses Verhalten. Nehmen Sie an, Sie konfigurieren eine Richtlinie für das Löschen von Konten und wenden sie auf einen bestimmten Container an. Im Allgemeinen wird die Richtlinie vom übergeordneten Container an untergeordnete Container übergeben. Sie wird also auf alle untergeordneten Container des jeweiligen übergeordneten Containers angewendet, und ActiveRoles Server löscht folglich deprovisionierte Benutzerkonten in allen diesen Containern. Wenn Sie jedoch eine andere Richtlinie konfigurieren, mit der Konten nicht gelöscht werden, und diese neue Richtlinie auf einen untergeordneten Container anwenden, setzt die Richtlinie des untergeordneten Containers die vom übergeordneten Container geerbte Richtlinie außer Kraft. ActiveRoles Server löscht dann keine deprovisionierten Benutzerkonten aus diesem untergeordneten Container oder den Containern darunter.

Eine weitere Option dieser Richtlinie gilt für Domänen, in denen die Active Directory-Papierkorbfunktion aktiviert ist. Die Richtlinie kann so konfiguriert werden, dass ein Benutzerkonto direkt nach seiner Deprovisionierung in den Papierkorb verschoben wird (was bedeutet, dass das Konto sofort und ohne jegliche Aufbewahrungsdauer gelöscht wird). Das Verschieben von deprovisionierten Benutzerkonten in den Papierkorb kann aus Sicherheitsgründen als zusätzliche Maßnahme erforderlich sein. Der Active Directory-Papierkorb gewährleistet, dass das Konto bei Bedarf ohne jeglichen Datenverlust wiederhergestellt werden kann. ActiveRoles Server bietet die Möglichkeit, das Löschen von Benutzerkonten, die in den Papierkorb deprovisioniert wurden, rückgängig zu machen und die Deprovision dann aufzuheben.

Konfigurieren der Richtlinie „Permanentes Löschen von Benutzerkonten“

Um die Richtlinie „Permanentes Löschen von Benutzerkonten“ zu konfigurieren, wählen Sie **Permanentes Löschen von Benutzerkonten** auf der Seite **Zu konfigurierende Richtlinie** im Assistenten „Neues Deprovisionsrichtlinienobjekt“ oder im Assistenten „Deprovisionsrichtlinie hinzufügen“ aus. Klicken Sie dann auf **Weiter**, damit die Seite **Löschoptionen** angezeigt wird.


Assistent für neues Richtlinienobjekt zur Bereitstellungsrücknahme
Löschoptionen
Sie können wählen, ob die Richtlinie deprovisionierte Objekte löschen soll.
Nach der Deprovision eines Objekts werden die gewählten Optionen auf das Objekt angewandt.
Objekt nicht automatisch löschen
Objekt nach der Aufbewahrungsdauer löschen
Aufbewahrungsdauer (Tage):
90
Objekt sofort in den Active Directory-Papierkorb verschieben
Diese Option hat nur dann einen Einfluss, wenn die Active Directory-Papierkorbfunktion in der Domäne des Objekts aktiviert ist.
< Zurück
Weiter >
Abbrechen
Hilfe

Auf dieser Seite können Sie auswählen, ob die Richtlinie für deprovisionierte Benutzerkonten die Löschung planen soll. Außerdem können Sie angeben, für wie viele Tage deprovisionierte Benutzerkonten beibehalten werden sollen.

Wählen Sie zunächst eine der folgenden Optionen aus:

- Klicken Sie auf **Objekt nicht automatisch löschen**, wenn die Richtlinie deprovisionierte Benutzerkonten nicht löschen soll.
- Klicken Sie auf **Objekt nach der Aufbewahrungsdauer löschen**, wenn die Richtlinie das Löschen von deprovisionierten Benutzerkonten planen soll.
- Klicken Sie auf **Objekt sofort in den Active Directory-Papierkorb verschieben**, wenn die Richtlinie deprovisionierte Benutzerkonten in den Papierkorb verschieben soll.

Wenn Sie die zweite Option auswählen, müssen Sie in dem Feld unter dieser Option eine Anzahl von Tagen angeben. Nachdem ein Benutzerkonto deprovisioniert wurde und die angegebene Anzahl von Tagen vergangen ist, löscht ActiveRoles Server aufgrund der Richtlinie das Benutzerkonto aus Active Directory.

Wenn Sie die dritte Option auswählen, sollten Sie diese Richtlinie auf Domänen anwenden, in denen der Active Directory-Papierkorb aktiviert ist; andernfalls hat die Richtlinie keine Auswirkungen. Bei Aktivierung dieser Option führt die Richtlinie, sobald ein Benutzerkonto deprovisioniert wurde, dazu, dass ActiveRoles Server das Benutzerkonto sofort löscht. In einer Domäne, in der der Active Directory-Papierkorb aktiviert ist, bedeutet dieser Löschvorgang bloß, dass das Konto als gelöscht markiert und in einen bestimmten Container verschoben wird, aus dem es bei Bedarf ohne Datenverlust wiederhergestellt werden kann.

Schrittweise Anleitungen finden Sie unter **Anleitungen/Verwalten von Richtlinienobjekten/ Konfigurieren von Deprovisionsrichtlinienobjekten/Konfigurieren einer Richtlinie zum permanenten Löschen von Benutzerkonten** in der ActiveRoles Server-Hilfe.

Szenario: Löschen deprovisionierter Benutzerkonten

In diesem Szenario wird beschrieben, wie Sie eine Richtlinie konfigurieren, damit ActiveRoles Server deprovisionierte Benutzerkonten nach einem Wartezeitraum von 90 Tagen dauerhaft löscht.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen und konfigurieren Sie das Richtlinienobjekt, das die entsprechende Richtlinie definiert.
2. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Nach der Deprovision für ein Benutzerkonto in dem Container, den Sie in Schritt 2 ausgewählt haben, behält ActiveRoles Server folglich dieses Konto für 90 Tage bei und löscht es dann.

Schritt 1: Erstellen und Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt mit dem Assistenten „Neues Deprovisionsrichtlinienobjekt" erstellen und konfigurieren. Weitere Informationen über den Assistenten finden Sie unter „Erstellen eines Richtlinienobjekts" im Abschnitt „Verwaltungsaufgaben für Richtlinienobjekte" weiter oben in diesem Kapitel.

Klicken Sie zum Konfigurieren der Richtlinie auf der Seite **Richtlinientyp auswählen** des Assistenten auf **Permanentes Löschen von Benutzerkonten**. Klicken Sie dann auf **Weiter**.

Klicken Sie auf der Seite **Löschoptionen** auf **Objekt nach der Aufbewahrungsdauer löschen**. Geben Sie dann in das Feld unter dieser Option den Wert **90** ein.

Klicken Sie nach Abschluss des Vorgangs auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schritt 2: Anwenden des Richtlinienobjekts

Sie können das Richtlinienobjekt mit Hilfe der Seite **Richtlinie erzwingen** im Assistenten „Neues Deprovisionsrichtlinienobjekt" anwenden oder Sie können den Assistenten erst abschließen und dann den Befehl **Richtlinie erzwingen** für die Domäne, die Organisationseinheit oder die verwaltete Einheit verwenden, auf die Sie die Richtlinie anwenden möchten.

Weitere Informationen über die Anwendung eines Richtlinienobjekts finden Sie unter „Anwenden von Richtlinienobjekten" und „Verwalten des Richtlinienbereichs" weiter oben in diesem Kapitel.

Gruppenobjekt-Deprovisionierung

Die Richtlinie zur Deprovisionierung von Gruppenobjekten gibt die Änderungen an, die am Gruppenobjekt in Active Directory vorzunehmen sind, um die Verwendung der Gruppe zu vermeiden. Sie dient zur Durchführung der folgenden Aufgaben im Rahmen der Deprovisionierung einer Gruppe:

- Ausblenden der Gruppe in der Globalen Adressliste (GAL), um den Zugriff auf die Gruppe ausgehend von Exchange Server-Client-Anwendungen wie etwa Microsoft Outlook zu verhindern.
- Ändern des Typs der Gruppe von „Sicherheit" in „Verteilung", um die Zugriffsrechte von dieser Gruppe zurückzuziehen.
- Umbenennen der Gruppe, um deprovisionierte Gruppen nach Namen unterscheiden zu können.
- Entfernen von Mitgliedern aus dieser Gruppe, um den Benutzerzugriff auf Ressourcen zu widerrufen, die von der Gruppe kontrolliert werden. Diese Aufgabe bietet die Möglichkeit zur Angabe der Mitglieder, die nicht aus der Gruppe entfernt werden sollen.

Darüber hinaus kann die Richtlinie so konfiguriert werden, dass sie jegliche andere Eigenschaften einer Gruppe wie etwa den Prä-Windows 2000-Namen, E-Mail-Adressen oder die Beschreibung ändert oder löscht.

Funktionsweise dieser Richtlinie

Beim Verarbeiten einer Deprovisionsanforderung für eine Gruppe verwendet ActiveRoles Server diese Richtlinie, um das Gruppenobjekt in Active Directory so zu ändern, dass die Gruppe nach ihrer Deprovisionierung nicht mehr verwendet werden kann.

Es kann auch eine Richtlinie zum Aktualisieren einzelner Eigenschaften der Gruppen konfiguriert werden. Abhängig von der Richtlinienkonfiguration hat jede richtlinienbasierte Aktualisierung folgende Ergebnisse:

- Bestimmte Abschnitte der Gruppeninformationen wie etwa die Informationen über Gruppenmitglieder werden aus dem Verzeichnis entfernt.
- Bestimmte Eigenschaften von Gruppen werden geändert oder gelöscht.

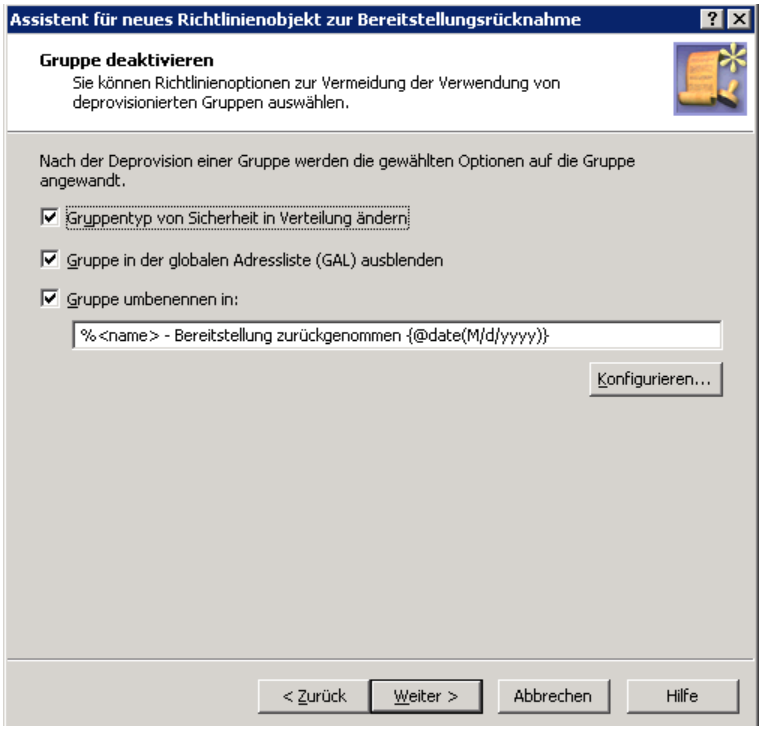
Eine Richtlinie kann so konfiguriert werden, dass sie folgende neue Eigenschaftswerte einschließt:

- Eigenschaften der Gruppe, für das die Bereitstellung zurückgenommen wird. Diese Eigenschaften wurden vor dem Beginn des Rücknahmevorgangs für die Gruppe aus dem Verzeichnis abgerufen
- Eigenschaften des Benutzers, der die Rücknahmeanforderung gestellt hat
- Datum und Uhrzeit der Deprovision der Gruppe

ActiveRoles Server ändert also bei der Deprovision einer Gruppe das Gruppenobjekt in Active Directory so, wie es von der gültigen Gruppenobjekt-Deprovisionierungsrichtlinie bestimmt wird.

Konfigurieren der Gruppenobjekt-Deprovisionierungsrichtlinie

Um eine Gruppenobjekt-Deprovisionierungsrichtlinie zu konfigurieren, wählen Sie **Gruppenobjekt-Deprovisionierung** auf der Seite **Zu konfigurierende Richtlinie** im Assistenten „Neues Deprovisionsrichtlinienobjekt" oder im Assistenten „Deprovisionsrichtlinie hinzufügen" aus. Klicken Sie dann auf **Weiter**, um die Seite **Gruppe deaktivieren** anzuzeigen:


Assistent für neues Richtlinienobjekt zur Bereitstellungsrücknahme
Gruppe deaktivieren
Sie können Richtlinienoptionen zur Vermeidung der Verwendung von deprovisionierten Gruppen auswählen.
Nach der Deprovision einer Gruppe werden die gewählten Optionen auf die Gruppe angewandt.
Gruppentyp von Sicherheit in Verteilung ändern
Gruppe in der globalen Adressliste (GAL) ausblenden
Gruppe umbenennen in:
%<name> - Bereitstellung zurückgenommen {@date(M/d/yyyy)}
Konfigurieren...
< Zurück
Weiter >
Abbrechen
Hilfe

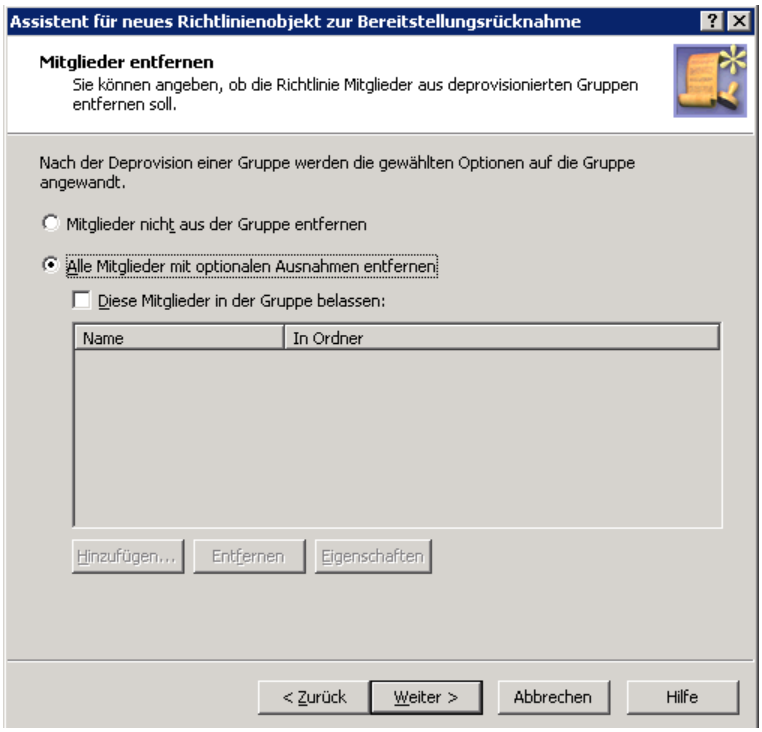
Auf dieser Seite können Sie unter den folgenden Optionen wählen:

- **Gruppentyp von „Sicherheit" in „Verteilung" ändern** Widerruft Zugriffsrechte von deprovisionierten Gruppen. Diese Option gilt nur für Sicherheitsgruppen.
- **Gruppe in der globalen Adressliste (GAL) ausblenden** Verhindert den Zugriff auf deprovisionierte Gruppen ausgehend von Exchange Server-Client-Anwendungen. Diese Option ist auf Verteilergruppen oder E-Mail-fähige Sicherheitsgruppen anwendbar.
- **Gruppe umbenennen in** Ändert den Namen der Gruppe.

Aktivieren Sie das Kontrollkästchen neben jeder Option, auf die die Richtlinie angewandt werden soll.

Durch Aktivieren des Kontrollkästchens **Gruppe umbenennen in** weisen Sie die Richtlinie an, den Namen der Gruppe zu ändern. Mit dieser Option können Sie eine *Eigenschaftsaktualisierungsregel* konfigurieren, die angibt, wie der Gruppenname geändert werden soll. Klicken Sie auf die Schaltfläche **Konfigurieren** und folgen Sie den Anweisungen im Abschnitt „Konfigurieren einer Eigenschaftsaktualisierungsregel" weiter oben in diesem Kapitel.

Wenn Sie die Seite **Gruppe deaktivieren** abgeschlossen haben, klicken Sie auf **Weiter**, um die Seite **Mitglieder entfernen** anzuzeigen:


Assistent für neues Richtlinienobjekt zur Bereitstellungsrücknahme
Mitglieder entfernen
Sie können angeben, ob die Richtlinie Mitglieder aus deprovisionierten Gruppen entfernen soll.
Nach der Deprovision einer Gruppe werden die gewählten Optionen auf die Gruppe angewandt.
Mitglieder nicht aus der Gruppe entfernen
Alle Mitglieder mit optionalen Ausnahmen entfernen
Diese Mitglieder in der Gruppe belassen:
Name
In Ordner
Hinzufügen...
Entfernen
Eigenschaften
< Zurück
Weiter >
Abbrechen
Hilfe

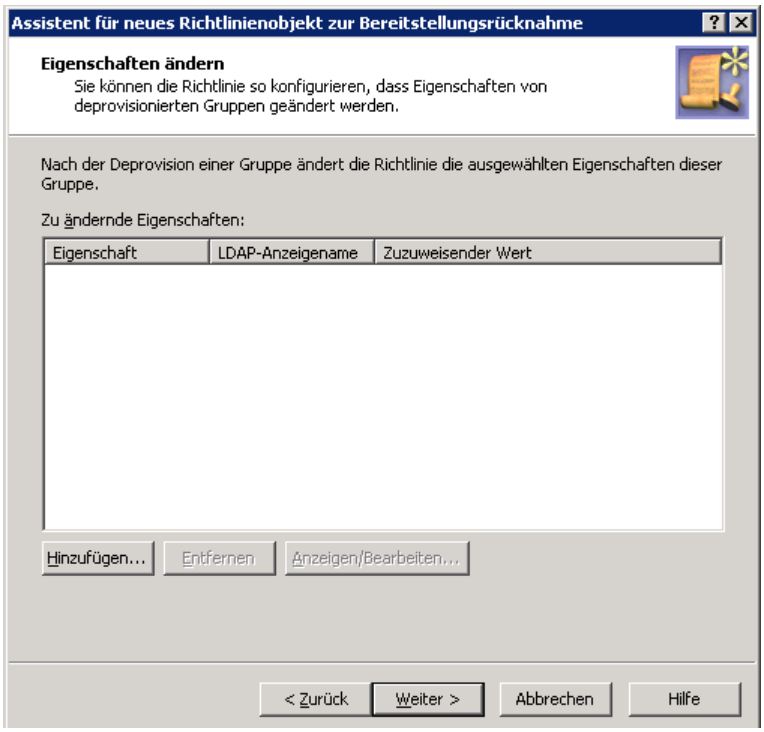
Auf dieser Seite können Sie eine Regel konfigurieren, die angibt, wie Mitglieder aus deprovisionierten Gruppen entfernt werden sollen.

Wählen Sie eine der folgenden Optionen aus:

- Klicken Sie auf **Mitglieder nicht aus der Gruppe entfernen**, wenn Sie möchten, dass die Richtlinie keine Mitglieder aus deprovisionierten Gruppen entfernen soll.
- Klicken Sie auf **Alle Mitglieder mit optionalen Ausnahmen entfernen**, wenn Sie möchten, dass die Richtlinie Mitglieder aus deprovisionierten Gruppen entfernen soll.

Mit der zweiten Option können Sie angeben, ob die Richtlinie bestimmte Objekte aus deprovisionierten Gruppen nicht entfernen soll. Um eine Liste solcher Objekte zu erstellen, aktivieren Sie das Kontrollkästchen **Diese Objekte in der Gruppe belassen**, klicken Sie dann auf die Schaltfläche **Hinzufügen** und wählen Sie die Objekte aus, die in die Liste aufgenommen werden sollen.

Wenn Sie die Seite **Mitglieder entfernen** abgeschlossen haben, klicken Sie auf **Weiter**, um die Seite **Eigenschaften ändern** anzuzeigen:



Auf dieser Seite können Sie eine Liste von Gruppeneigenschaften einrichten, die die Richtlinie aktualisieren soll. Jeder Eintrag in der Liste schließt die folgenden Informationen ein:

- **Eigenschaft** Bei der Deprovisionierung einer Gruppe aktualisiert ActiveRoles Server diese Eigenschaft des Gruppenobjekts in Active Directory.
- **LDAP-Anzeigename** Identifiziert die zu aktualisierende Eigenschaft eindeutig.
- **Zuzuweisender Wert** Nach dem Abschluss des Deprovisionsvorgangs besitzt die Eigenschaft den durch die angegebene Regel definierten Wert.

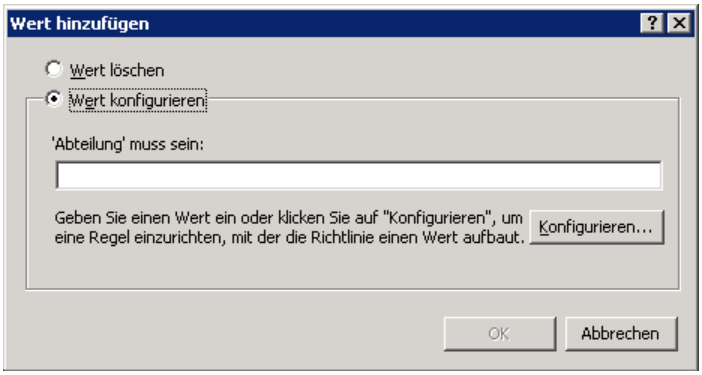
Sie können die Liste auf dieser Seite mit folgenden Schaltflächen verwalten:

- **Hinzufügen** Ermöglicht das Auswählen einer Eigenschaft und das Konfigurieren einer Aktualisierungsregel für diese Eigenschaft. Eine Eigenschaftsaktualisierungsregel gibt an, wie der neue Wert generiert werden soll, der der Eigenschaft zugewiesen wird.
- **Entfernen** Wenn die Richtlinie eine bestimmte Eigenschaft nicht mehr aktualisieren soll, wählen Sie die Eigenschaft in der Liste aus und klicken Sie auf **Entfernen**.
- **Anzeigen/Bearbeiten** Ermöglicht das Ändern der Aktualisierungsregel für die Eigenschaft, die Sie in der Liste auswählen.

Wenn Sie auf die Schaltfläche **Hinzufügen** klicken, wird das Dialogfeld **Objekteigenschaft wählen** angezeigt. In diesem Dialogfeld können Sie Gruppeneigenschaften auswählen, die die Richtlinie aktualisieren soll. Um eine Eigenschaft auszuwählen, aktivieren Sie das Kontrollkästchen neben dem Eigenschaftsnamen und klicken Sie dann auf **OK**.

Sie können mehrere Kontrollkästchen aktivieren. In diesem Fall werden die ausgewählten Eigenschaften der Liste auf der Seite des Assistenten hinzugefügt, und die Aktualisierungsregel wird so konfiguriert, dass sie diese Eigenschaften löscht, ihnen also den „leeren" Wert zuweist.

Wenn Sie eine einzelne Eigenschaft im Dialogfeld **Objekteigenschaft auswählen** auswählen, wird das Dialogfeld **Wert hinzufügen** angezeigt, sodass Sie den Vorgang mit der Konfiguration einer Eigenschafts-Aktualisierungsregel fortsetzen können:


Wert hinzufügen
Wert löschen
Wert konfigurieren
'Abteilung' muss sein:
Geben Sie einen Wert ein oder klicken Sie auf "Konfigurieren", um eine Regel einzurichten, mit der die Richtlinie einen Wert aufbaut.
Konfigurieren...
OK
Abbrechen

Sie können eine der folgenden Aktualisierungsoptionen auswählen:

- **Wert löschen** Veranlasst die Richtlinie dazu, der Eigenschaft den „leeren" Wert zuzuweisen.
- **Wert konfigurieren** Ermöglicht das Konfigurieren eines Wertes für die Bedingung **„Eigenschaft" muss sein**.

Bei der zweiten Option müssen Sie einen Wert konfigurieren, den die Richtlinie bei der Deprovision einer Gruppe der Eigenschaft zuweisen soll. Sie können einen Wert auf die gleiche Weise konfigurieren wie beim Konfigurieren einer Eigenschaftsaktualisierungsregel für den Benutzernamen: Klicken Sie auf die Schaltfläche **Konfigurieren** und folgen Sie den Anweisungen im Abschnitt „Konfigurieren einer Eigenschaftsaktualisierungsregel" weiter oben in diesem Kapitel.

Klicken Sie nach dem Konfigurieren eines Wertes auf **OK**, um das Dialogfeld **Wert hinzufügen** zu schließen. Der Eigenschaftsname wird zusammen mit der Eigenschaftsaktualisierungsregel der Seite des Assistenten hinzugefügt. Nötigenfalls können Sie die Aktualisierungsregel ändern, indem Sie unter der Eigenschaftenliste auf die Schaltfläche **Anzeigen/Bearbeiten** klicken. Dann wird ein Dialogfeld angezeigt, das dem Dialogfeld **Wert hinzufügen** ähnelt und in dem Sie eine andere Aktualisierungsoption auswählen oder einen anderen Wert für die Bedingung **„Eigenschaft" muss sein** festlegen können.

Klicken Sie nach dem Einrichten der Liste auf der Seite des Assistenten auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schrittweise Anleitungen finden Sie unter **Anleitungen/Verwalten von Richtlinienobjekten/ Konfigurieren von Deprovisionsrichtlinienobjekten/Konfigurieren einer Gruppenobjekt-Deprovisionierungsrichtlinie** in der ActiveRoles Server-Hilfe.

Szenario 1: Deaktivieren und Umbenennen von Gruppen bei der Deprovision der Gruppe

Die in diesem Szenario beschriebene Richtlinie führt während der Deprovision für eine Gruppe die folgenden Funktionen aus:

- Bei der Deprovisionierung einer Sicherheitsgruppe Änderung des Gruppentyps in „Verteilung".
- Bei der Deprovisionierung einer Verteilergruppe Entfernung der Gruppe aus der Globalen Adressliste.
- Anhängen des folgenden Suffix an den Gruppennamen: **- Deprovisioniert**, gefolgt von dem Datum, an dem die Gruppe deprovisioniert wurde.

Beispielsweise ändert die Richtlinie den Gruppennamen von **Partner Marketing** in **Partner Marketing – Deprovisioniert am 12/11/2009** um.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen und konfigurieren Sie das Richtlinienobjekt, das die entsprechende Richtlinie definiert.
2. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Bei der Deprovisionierung einer Gruppe in dem Container, den Sie in Schritt 2 ausgewählt haben, deaktiviert ActiveRoles Server folglich die Gruppe und benennt sie wie von dieser Richtlinie vorgeschrieben um.

In den folgenden beiden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen und Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt mit dem Assistenten „Neues Deprovisionsrichtlinienobjekt" erstellen und konfigurieren. Weitere Informationen über den Assistenten finden Sie unter „Erstellen eines Richtlinienobjekts" im Abschnitt „Verwaltungsaufgaben für Richtlinienobjekte" weiter oben in diesem Kapitel.

Um die Richtlinie zu konfigurieren, klicken Sie auf **Gruppenobjekt-Deprovisionierung** auf der Seite **Richtlinientyp auswählen** des Assistenten. Klicken Sie dann auf **Weiter**.

Aktivieren Sie auf der Seite **Gruppe deaktivieren** die folgenden Kontrollkästchen:

- **Gruppentyp von „Sicherheit" in „Verteilung" ändern**
- **Gruppe in der globalen Adressliste (GAL) ausblenden**
- **Gruppe umbenennen in**

Geben Sie dann den folgenden Text in das Feld unter der Option **Gruppe umbenennen in** ein:

```
%<name> - Deprovisioned {@date(M/d/yyyy)}
```

Klicken Sie auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schritt 2: Anwenden des Richtlinienobjekts

Sie können das Richtlinienobjekt mit Hilfe der Seite **Richtlinie erzwingen** im Assistenten „Neues Deprovisionsrichtlinienobjekt" anwenden oder Sie können den Assistenten erst abschließen und dann den Befehl **Richtlinie erzwingen** für die Domäne, die Organisationseinheit oder die verwaltete Einheit verwenden, auf die Sie die Richtlinie anwenden möchten.

Weitere Informationen über die Anwendung eines Richtlinienobjekts finden Sie unter „Anwenden von Richtlinienobjekten" und „Verwalten des Richtlinienbereichs" weiter oben in diesem Kapitel.

Szenario 2: Verwaltete Einheit zum Ablegen deprovisionierter Gruppen

In diesem Szenario wird beschrieben, wie Sie eine verwaltete Einheit und eine Gruppenobjekt-Deprovisionierungsrichtlinie so konfigurieren, dass die verwaltete Einheit alle deprovisionierten Gruppen enthält. Die Richtlinie setzt bei der Deprovisionierung einer Gruppe die Eigenschaft **Hinweise** auf **Deprovisioniert**. Die verwaltete Einheit wiederum ist so konfiguriert, dass sie die Gruppen einschließt, deren Eigenschaft **Hinweise** auf **Stillgelegt** gesetzt ist.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen und konfigurieren Sie die verwaltete Einheit.
2. Konfigurieren Sie das Richtlinienobjekt, das die entsprechende Richtlinie definiert.
3. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Nach der Deprovision einer Gruppe in dem Container, den Sie in Schritt 3 ausgewählt haben, fügt ActiveRoles Server folglich diese Gruppe automatisch zu der in Schritt 1 erstellten verwalteten Einheit hinzu.

In den folgenden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen und Konfigurieren der verwalteten Einheit

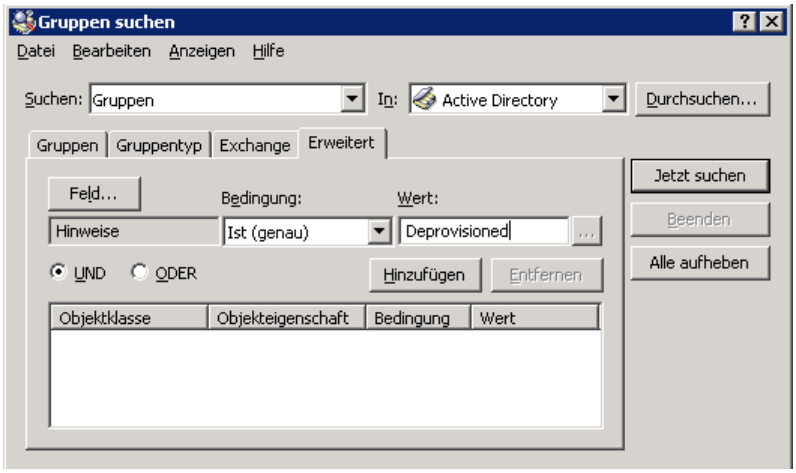
Sie können die verwaltete Einheit mittels der ActiveRoles Server-Konsole erstellen und konfigurieren:

1. Klicken Sie in der Konsolenstruktur unter **Configuration** mit der rechten Maustaste auf **Verwaltete Einheiten**, und wählen Sie **Neu | Verwaltete Einheit** aus.
2. Geben Sie in das Feld **Name** einen Namen für die verwaltete Einheit ein. Sie können beispielsweise **Deprovisionierte Gruppen** eingeben.
3. Klicken Sie auf **Weiter**.
4. Konfigurieren Sie wie folgt die Mitgliedschaftsregel so, dass die verwaltete Einheit die deprovisionierten Gruppenobjekte aus allen bei ActiveRoles Server registrierten Domänen (den verwalteten Domänen) enthält:
   a) Klicken Sie auf der Seite des Assistenten auf **Hinzufügen**.
   b) Klicken Sie im Dialogfeld **Mitgliedschaftsregeltyp** auf **Nach Abfrage einschließen** und klicken Sie dann auf **OK**.

c) Richten Sie im Fenster **Mitgliedschaftsregel erstellen** die Regel ein:

- Klicken Sie unter **Suchen** auf **Gruppen**.
- Klicken Sie auf **Durchsuchen** und wählen Sie **Active Directory** aus.
- Klicken Sie auf die Registerkarte **Erweitert**.
- Klicken Sie auf die Schaltfläche **Feld** und dann auf **Hinweise**.
- Klicken Sie unter **Bedingung** auf **Ist (genau)**.
- Geben Sie unter **Wert** den Wert **Deprovisioniert** ein.

Nun sollte das Fenster der folgenden Abbildung entsprechen:



- Klicken Sie auf die Schaltfläche **Hinzufügen**.
- Klicken Sie auf die Schaltfläche **Regel hinzufügen**.

d) Klicken Sie auf der Seite des Assistenten auf **Hinzufügen**.

e) Klicken Sie im Dialogfeld **Mitgliedschaftsregeltyp** auf **Deprovisionierte beibehalten** und klicken Sie dann auf **OK**.

5. Klicken Sie auf **Weiter**, wiederum auf **Weiter** und dann auf **Fertig stellen**.

Schritt 2: Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt konfigurieren, indem Sie das Richtlinienobjekt ändern, das das vorige Szenario implementiert; siehe „Szenario 1: Deaktivieren und Umbenennen von Gruppen bei der Gruppendeprovisionierung" weiter oben in diesem Abschnitt.

Zeigen Sie das Dialogfeld **Eigenschaften** für dieses Richtlinienobjekt an und öffnen Sie die Registerkarte **Richtlinien**. Wählen Sie dann die Richtlinie aus der Liste aus und klicken Sie dann auf **Anzeigen/ Bearbeiten**, um das Dialogfeld **Eigenschaften der Gruppenobjekt-Deprovisionierungsrichtlinie** anzuzeigen. Klicken Sie auf die Registerkarte **Eigenschaften ändern**.

Die Registerkarte **Eigenschaften ändern** ähnelt der Seite mit demselben Namen in dem Assistenten, den Sie für die Erstellung des Richtlinienobjekts verwenden. Mit dieser Registerkarte können Sie wie folgt die Aktualisierungsregel für die Eigenschaft **Hinweise** hinzufügen:

1. Klicken Sie auf **Hinzufügen**, um das Dialogfeld **Objekteigenschaft wählen** anzuzeigen.
2. Aktivieren Sie das Kontrollkästchen neben der Eigenschaft **Hinweise** und klicken Sie dann auf **OK**.
3. Geben Sie im Dialogfeld **Wert hinzufügen** in das Feld **„Hinweise" muss sein** den Wert **Deprovisioniert** ein und klicken Sie dann auf **OK**.

Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften der Gruppenobjekt-Deprovisionierungs-richtlinie** zu schließen.

Schritt 3: Anwenden des Richtlinienobjekts

Um das Richtlinienobjekt anzuwenden, können Sie im Dialogfeld **Eigenschaften** für dieses Richtlinienobjekt die Registerkarte **Bereich** verwenden:

1. Klicken Sie auf der Registerkarte **Bereich** auf die Schaltfläche **Bereich**, um das Fenster **ActiveRoles Serverrichtlinienbereich** für das zu verwaltende Richtlinienobjekt anzuzeigen.
2. Klicken Sie auf **Hinzufügen** und wählen Sie die Domäne, Organisationseinheit oder verwaltete Einheit aus, auf die Sie die Richtlinie anwenden möchten.
3. Klicken Sie auf **OK**, um das Fenster **ActiveRoles Serverrichtlinienbereich** zu schließen.
4. Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften** für das Richtlinienobjekt zu schließen.

Weitere Informationen über die Anwendung eines Richtlinienobjekts finden Sie unter „Anwenden von Richtlinienobjekten" und „Verwalten des Richtlinienbereichs" weiter oben in diesem Kapitel.

Gruppenobjekt-Verschiebung

Richtlinien dieser Kategorie dienen zum Automatisieren der Verschiebung von deprovisionierten Gruppenobjekten in angegebene Organisationseinheiten. So werden solche Gruppen der Steuerung der Administratoren entzogen, die die Organisationseinheiten verwalten, in denen sich diese Gruppen ursprünglich befanden. Eine Richtlinie dieser Kategorie kann auch so konfiguriert werden, dass sie deprovisionierte Gruppenobjekte nicht verschiebt.

Funktionsweise dieser Richtlinie

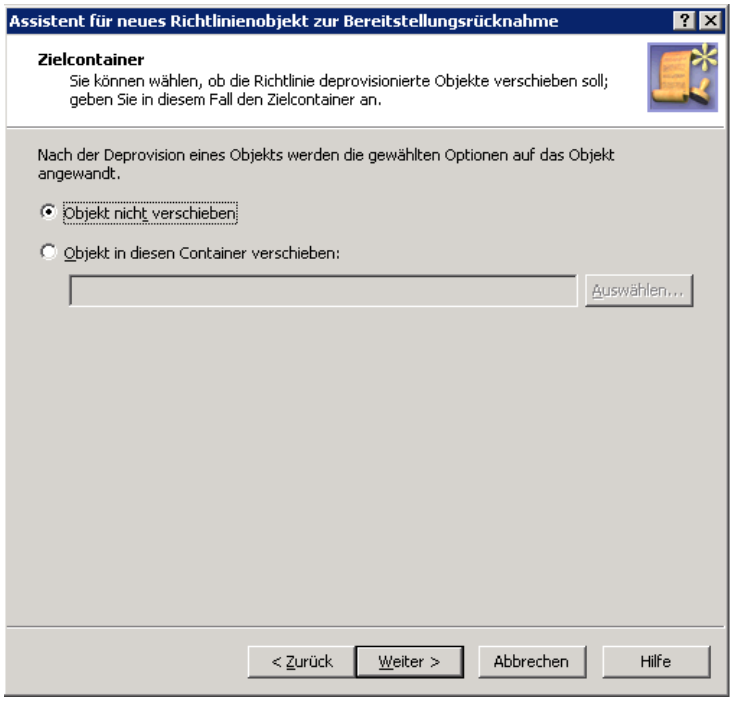
Beim Verarbeiten einer Deprovisionsanforderung für eine Gruppe verwendet ActiveRoles Server diese Richtlinie, um zu bestimmen, ob das deprovisionierte Gruppenobjekt in eine andere Organisationseinheit verschoben werden soll.

Eine für das Verschieben von Gruppenobjekten konfigurierte Richtlinie gibt auch das Ziel an, also die Organisationseinheit, in die ActiveRoles Server deprovisionierte Gruppenobjekte verschiebt.

Es kann auch eine Richtlinie konfiguriert werden, die Gruppenobjekte nicht verschiebt. Wenn eine solche Richtlinie auf einer bestimmten Ebene der Verzeichnishierarchie angewendet wird, setzt sie ggf. alle anderen Richtlinien diese Kategorie außer Kraft, die auf einer höheren Ebene der Verzeichnishierarchie angewendet werden.

Gehen Sie folgendermaßen vor, um eine Richtlinie zum Verschieben von Gruppenobjekten zu konfigurieren

Um eine Richtlinie zum Verschieben von Gruppenobjekten zu konfigurieren, wählen Sie **Gruppenobjekt-Verschiebung** auf der Seite **Zu konfigurierende Richtlinie** im Assistenten „Neues Deprovisionsrichtlinienobjekt" oder im Assistenten „Deprovisionsrichtlinie hinzufügen" aus. Klicken Sie dann auf **Weiter**, damit die Seite **Zielcontainer** angezeigt wird.


Assistent für neues Richtlinienobjekt zur Bereitstellungsrücknahme
Zielcontainer
Sie können wählen, ob die Richtlinie deprovisionierte Objekte verschieben soll; geben Sie in diesem Fall den Zielcontainer an.
Nach der Deprovision eines Objekts werden die gewählten Optionen auf das Objekt angewandt.
Objekt nicht verschieben
Objekt in diesen Container verschieben:
Auswählen...
< Zurück
Weiter >
Abbrechen
Hilfe

Auf dieser Seite können Sie auswählen, ob die Richtlinie deprovisionierte Gruppenobjekte verschieben soll, und Sie können den Zielcontainer für den Verschiebungsvorgang auswählen.

Wählen Sie zunächst eine der folgenden Optionen aus:

- Klicken Sie auf **Objekt nicht verschieben**, damit die Richtlinie deprovisionierte Gruppenobjekte an ihren ursprünglichen Orten belässt. Mit dieser Option verbleibt jedes deprovisionierte Gruppenobjekt in der Organisationseinheit, in der es sich bei der Deprovisionierung befand.
- Klicken Sie auf **Objekt in diesen Container verschieben**, damit die Richtlinie deprovisionierte Gruppenobjekte in einen bestimmten Container verschiebt. Mit dieser Option wird jedes deprovisionierte Gruppenobjekt von seinem ursprünglichen Ort in eine angegebene Organisationseinheit verschoben.

Für die zweite Option müssen Sie die Organisationseinheit angeben, in die die Richtlinie deprovisionierte Gruppenobjekte verschieben soll. Klicken Sie auf die Schaltfläche **Auswählen** und wählen Sie dann die gewünschte Organisationseinheit aus.

Klicken Sie nach Abschluss des Vorgangs auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schrittweise Anleitungen finden Sie unter **Anleitungen/Verwalten von Richtlinienobjekten/ Konfigurieren von Deprovisionsrichtlinienobjekten/Konfigurieren einer Richtlinie zum Verschieben von Gruppenobjekten** in der ActiveRoles Server-Hilfe.

Szenario: Organisationseinheit zum Ablegen deprovisionierter Gruppen

In diesem Szenario wird das Konfigurieren einer Richtlinie beschrieben, die dazu führt, dass eine bestimmte Organisationseinheit alle deprovisionierten Gruppen enthält.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen und konfigurieren Sie das Richtlinienobjekt, das die entsprechende Richtlinie definiert.
2. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Nach der Deprovision für eine Gruppe in dem Container, die Sie in Schritt 2 ausgewählt haben, verschiebt ActiveRoles Server folglich diese Gruppe automatisch in die von der Richtlinienkonfiguration bestimmte Organisationseinheit. In den folgenden beiden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen und Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt mit dem Assistenten „Neues Deprovisionsrichtlinienobjekt" erstellen und konfigurieren. Weitere Informationen über den Assistenten finden Sie unter „Erstellen eines Richtlinienobjekts" im Abschnitt „Verwaltungsaufgaben für Richtlinienobjekte" weiter oben in diesem Kapitel.

Um die Richtlinie zu konfigurieren, klicken Sie auf **Gruppenobjekt-Verschiebung** auf der Seite **Richtlinientyp auswählen** des Assistenten. Klicken Sie dann auf **Weiter**.

Klicken Sie auf der Seite **Zielcontainer** auf **Objekt in diesen Container verschieben**. Klicken Sie dann auf die Schaltfläche **Auswählen**, um das Dialogfeld **Container suchen** anzuzeigen. Suchen Sie die Organisationseinheit, in die die Richtlinie deprovisionierte Gruppen verschieben soll, und wählen Sie sie aus. Klicken Sie dann auf **OK**.

Klicken Sie nach Abschluss des Vorgangs auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schritt 2: Anwenden des Richtlinienobjekts

Sie können das Richtlinienobjekt mit Hilfe der Seite **Richtlinie erzwingen** im Assistenten „Neues Deprovisionsrichtlinienobjekt" anwenden oder Sie können den Assistenten erst abschließen und dann den Befehl **Richtlinie erzwingen** für die Domäne, die Organisationseinheit oder die verwaltete Einheit verwenden, auf die Sie die Richtlinie anwenden möchten.

Weitere Informationen über die Anwendung eines Richtlinienobjekts finden Sie unter „Anwenden von Richtlinienobjekten" und „Verwalten des Richtlinienbereichs" weiter oben in diesem Kapitel.

Dauerhaftes Löschen des Gruppenobjekts

Richtlinien dieser Kategorie dienen zum Automatisieren der Löschung von deprovisionierten Gruppen. Deprovisionierte Gruppenobjekte werden für einen angegebenen Zeitraum beibehalten, bevor sie dauerhaft gelöscht werden. Eine Richtlinie dieser Kategorie kann auch so konfiguriert werden, dass sie deprovisionierte Gruppenobjekte nicht löscht.

Funktionsweise dieser Richtlinie

Beim Verarbeiten einer Deprovisionsanforderung für eine Gruppe verwendet ActiveRoles Server diese Richtlinie, um zu bestimmen, ob für das deprovisionierte Gruppenobjekt die Löschung geplant werden soll. Ein Gruppenobjekt, für das die Löschung geplant ist, wird nach einem bestimmten Zeitraum dauerhaft gelöscht. Dieser wird als *Wartezeitraum* bezeichnet.

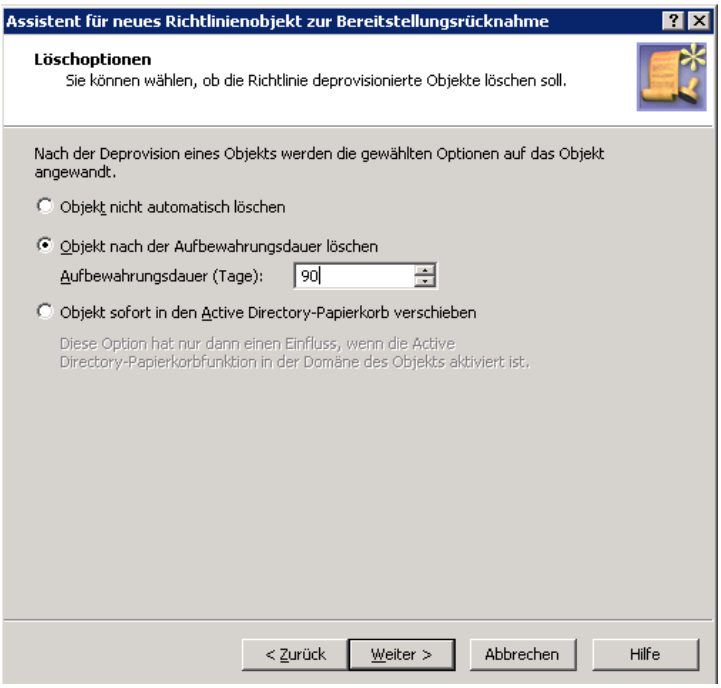
Eine Richtlinie, die zum Löschen von Gruppen konfiguriert ist, gibt an, für wie viele Tage deprovisionierte Gruppenobjekte beibehalten werden sollen. Mit einer solchen Richtlinie löscht ActiveRoles Server eine Gruppe nach der angegebenen Anzahl von Tagen seit der Deprovision für die Gruppe dauerhaft.

Es kann auch eine Richtlinie konfiguriert werden, die Gruppen nicht löscht. Wenn eine solche Richtlinie auf einer bestimmten Ebene der Verzeichnishierarchie angewendet wird, setzt sie ggf. alle anderen Richtlinien diese Kategorie außer Kraft, die auf einer höheren Ebene der Verzeichnishierarchie angewendet werden.

Eine weitere Option dieser Richtlinie gilt für Domänen, in denen die Active Directory-Papierkorbfunktion aktiviert ist. Die Richtlinie kann so konfiguriert werden, dass ein Gruppenobjekt direkt nach der Deprovisionierung der Gruppe in den Papierkorb verschoben wird (was bedeutet, dass die Gruppe sofort und ohne jegliche Aufbewahrungsdauer gelöscht wird). Das Verschieben von deprovisionierten Gruppenobjekten in den Papierkorb kann aus Sicherheitsgründen als zusätzliche Maßnahme erforderlich sein. Der Active Directory-Papierkorb gewährleistet, dass das Gruppenobjekt bei Bedarf ohne jeglichen Datenverlust wiederhergestellt werden kann. ActiveRoles Server bietet die Möglichkeit, das Löschen von Gruppen, die in den Papierkorb deprovisioniert wurden, rückgängig zu machen und die Deprovision dann aufzuheben.

Gehen Sie folgendermaßen vor, um eine Richtlinie zum permanenten Löschen eines Gruppenobjekts zu konfigurieren

Um eine Richtlinie zum permanenten Löschen eines Gruppenobjekts zu konfigurieren, wählen Sie **Dauerhaftes Löschen des Gruppenobjekts** auf der Seite **Zu konfigurierende Richtlinie** im Assistenten „Neues Deprovisionsrichtlinienobjekt" oder im Assistenten „Deprovisionsrichtlinie hinzufügen" aus. Klicken Sie dann auf **Weiter**, damit die Seite **Löschoptionen** angezeigt wird.


Assistent für neues Richtlinienobjekt zur Bereitstellungsrücknahme
Löschoptionen
Sie können wählen, ob die Richtlinie deprovisionierte Objekte löschen soll.
Nach der Deprovision eines Objekts werden die gewählten Optionen auf das Objekt angewandt.
Objekt nicht automatisch löschen
Objekt nach der Aufbewahrungsdauer löschen
Aufbewahrungsdauer (Tage):
90
Objekt sofort in den Active Directory-Papierkorb verschieben
Diese Option hat nur dann einen Einfluss, wenn die Active Directory-Papierkorbfunktion in der Domäne des Objekts aktiviert ist.
< Zurück
Weiter >
Abbrechen
Hilfe

Auf dieser Seite können Sie auswählen, ob die Richtlinie für deprovisionierte Gruppen die Löschung planen soll. Außerdem können Sie angeben, für wie viele Tage deprovisionierte Gruppen beibehalten werden sollen.

Wählen Sie zunächst eine der folgenden Optionen aus:

- Klicken Sie auf **Objekt nicht automatisch löschen**, wenn die Richtlinie deprovisionierte Gruppen nicht löschen soll.
- Klicken Sie auf **Objekt nach der Aufbewahrungsdauer löschen**, wenn die Richtlinie das Löschen von deprovisionierten Gruppen planen soll.
- Klicken Sie auf **Objekt sofort in den Active Directory-Papierkorb verschieben**, wenn die Richtlinie deprovisionierte Gruppenobjekte in den Papierkorb verschieben soll.

Wenn Sie die zweite Option auswählen, müssen Sie in dem Feld unter dieser Option eine Anzahl von Tagen angeben. Nachdem eine Gruppe deprovisioniert wurde und die angegebene Anzahl von Tagen vergangen ist, löscht ActiveRoles Server aufgrund der Richtlinie das Gruppenobjekt aus Active Directory.

Wenn Sie die dritte Option auswählen, sollten Sie diese Richtlinie auf Domänen anwenden, in denen der Active Directory-Papierkorb aktiviert ist; andernfalls hat die Richtlinie keine Auswirkungen. Bei Aktivierung dieser Option führt die Richtlinie, sobald eine Gruppe deprovisioniert wurde, dazu, dass ActiveRoles Server das Gruppenobjekt sofort löscht. In einer Domäne, in der der Active Directory-Papierkorb aktiviert ist, bedeutet dieser Löschvorgang bloß, dass das Objekt als gelöscht markiert und in einen bestimmten Container verschoben wird, aus dem es bei Bedarf ohne Datenverlust wiederhergestellt werden kann.

Schrittweise Anleitungen finden Sie unter **Anleitungen/Verwalten von Richtlinienobjekten/ Konfigurieren von Deprovisionsrichtlinienobjekten/Konfigurieren einer Richtlinie zum permanenten Löschen eines Gruppenobjekts** in der ActiveRoles Server-Hilfe.

Szenario: Löschen von deprovisionierten Gruppen

In diesem Szenario wird beschrieben, wie Sie eine Richtlinie konfigurieren, damit ActiveRoles Server deprovisionierte Gruppen nach einem Wartezeitraum von 90 Tagen dauerhaft löscht.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen und konfigurieren Sie das Richtlinienobjekt, das die entsprechende Richtlinie definiert.
2. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Nach der Deprovision einer Gruppe in dem Container, den Sie in Schritt 2 ausgewählt haben, behält ActiveRoles Server folglich das deprovisionierte Gruppenobjekt für 90 Tage bei und löscht das Objekt dann.

Schritt 1: Erstellen und Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt mit dem Assistenten „Neues Deprovisionsrichtlinienobjekt" erstellen und konfigurieren. Weitere Informationen über den Assistenten finden Sie unter „Erstellen eines Richtlinienobjekts" im Abschnitt „Verwaltungsaufgaben für Richtlinienobjekte" weiter oben in diesem Kapitel.

Um die Richtlinie zu konfigurieren, klicken Sie auf **Dauerhaftes Löschen des Gruppenobjekts** auf der Seite **Richtlinientyp auswählen** des Assistenten. Klicken Sie dann auf **Weiter**.

Klicken Sie auf der Seite **Löschoptionen** auf **Objekt nach der Aufbewahrungsdauer löschen**. Geben Sie dann in das Feld unter dieser Option den Wert **90** ein.

Klicken Sie nach Abschluss des Vorgangs auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schritt 2: Anwenden des Richtlinienobjekts

Sie können das Richtlinienobjekt mit Hilfe der Seite **Richtlinie erzwingen** im Assistenten „Neues Deprovisionsrichtlinienobjekt" anwenden oder Sie können den Assistenten erst abschließen und dann den Befehl **Richtlinie erzwingen** für die Domäne, die Organisationseinheit oder die verwaltete Einheit verwenden, auf die Sie die Richtlinie anwenden möchten.

Weitere Informationen über die Anwendung eines Richtlinienobjekts finden Sie unter „Anwenden von Richtlinienobjekten" und „Verwalten des Richtlinienbereichs" weiter oben in diesem Kapitel.

Benachrichtigungsverteilung

Mit Richtlinien dieser Kategorie werden bei eingehenden Deprovisionierungsanforderungen automatisch E-Mail-Benachrichtigungen generiert und versendet. Der primäre Zweck einer solchen Richtlinie ist die Benachrichtigung ausgewählter Personen über die Deprovisionsanforderung für ein bestimmtes Objekt, damit sie notfalls entsprechende Aktionen ausführen können. Beim Konfigurieren einer Richtlinie dieser Kategorie können Sie eine Liste von Benachrichtigungsempfängern angeben. Außerdem können Sie Betreff und Text der Benachrichtigung anpassen.

Funktionsweise dieser Richtlinie

Beim Verarbeiten einer Deprovisionsanforderung verwendet ActiveRoles Server diese Richtlinie, um zu bestimmen, ob andere Personen über den angeforderten Deprovisionsvorgang informiert werden müssen. Dann generiert ActiveRoles Server ggf. eine Benachrichtigung und versendet sie an die Empfänger, die in der Richtlinienkonfiguration angegeben wurden.

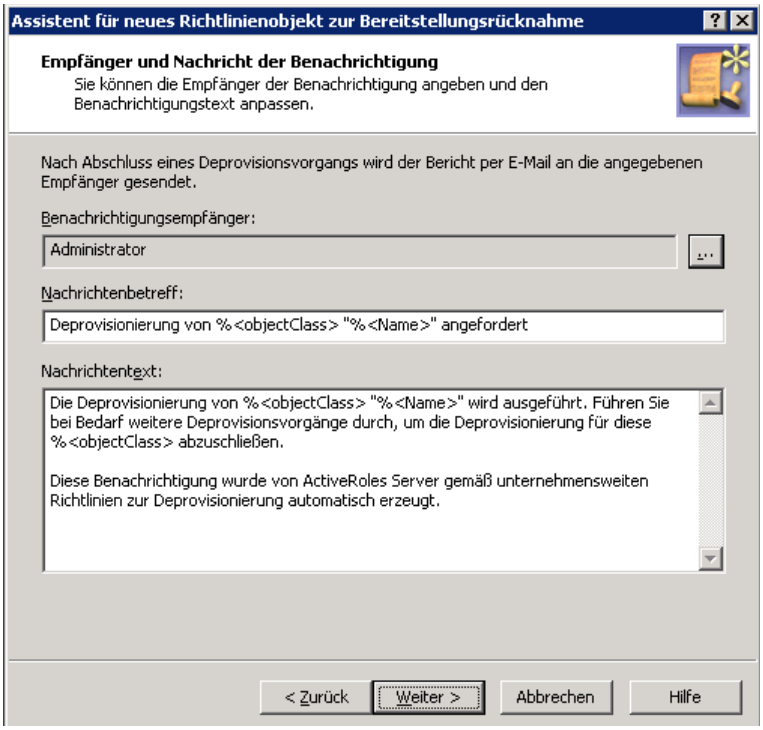
Wenn ein Deprovisionsvorgang angefordert wird, gibt ActiveRoles Server unabhängig von den Vorgangsergebnissen eine Benachrichtigung aus. Daher stellt das Vorliegen einer Benachrichtigung keine Aussage über Erfolg oder Fehler des Vorgangs dar. Sie gibt statt dessen nur an, dass die Deprovisionierung angefordert wurde. Wenn Personen über die Ergebnisse der Deprovision informiert werden sollen, sollten Sie die Richtlinie „Berichtsverteiler" verwenden, die im nächsten Abschnitt erörtert wird.

Die Benachrichtigungen werden pro Objekt ausgeführt: Jede Benachrichtigung enthält Informationen zu der Deprovisionsanforderung für ein einzelnes Objekt. Bei der Deprovision mehrerer Objekte versendet ActiveRoles Server mehrere Benachrichtigungen, eine pro Objekt.

ActiveRoles Server sendet die Benachrichtigungen über einen SMTP-Server. Die Richtlinienkonfiguration gibt den SMTP-Server für ausgehende Nachrichten mit Hilfe von ActiveRoles Server-E-Mail-Einstellungen an, die den Namen des SMTP-Servers sowie für die Verbindungsherstellung notwendige Informationen enthalten.

Konfigurieren der Richtlinie „Benachrichtigungsverteilung“

Um die Richtlinie „Benachrichtigungsverteilung“ zu konfigurieren, wählen Sie **Benachrichtigungsverteilung** auf der Seite **Zu konfigurierende Richtlinie** im Assistenten „Neues Deprovisionsrichtlinienobjekt“ oder im Assistenten „Deprovisionsrichtlinie hinzufügen“ aus. Klicken Sie dann auf **Weiter**, damit die Seite **Empfänger und Nachricht der Benachrichtigung** angezeigt wird.


Assistent für neues Richtlinienobjekt zur Bereitstellungsrücknahme
Empfänger und Nachricht der Benachrichtigung
Sie können die Empfänger der Benachrichtigung angeben und den Benachrichtigungstext anpassen.
Nach Abschluss eines Deprovisionsvorgangs wird der Bericht per E-Mail an die angegebenen Empfänger gesendet.
Benachrichtigungsempfänger:
Administrator
Nachrichtenbetreff:
Deprovisionierung von %<objectClass> "%<Name>" angefordert
Nachrichtentext:
Die Deprovisionierung von %<objectClass> "%<Name>" wird ausgeführt. Führen Sie bei Bedarf weitere Deprovisionsvorgänge durch, um die Deprovisionierung für diese %<objectClass> abzuschließen.
Diese Benachrichtigung wurde von ActiveRoles Server gemäß unternehmensweiten Richtlinien zur Deprovisionierung automatisch erzeugt.
< Zurück
Weiter >
Abbrechen
Hilfe

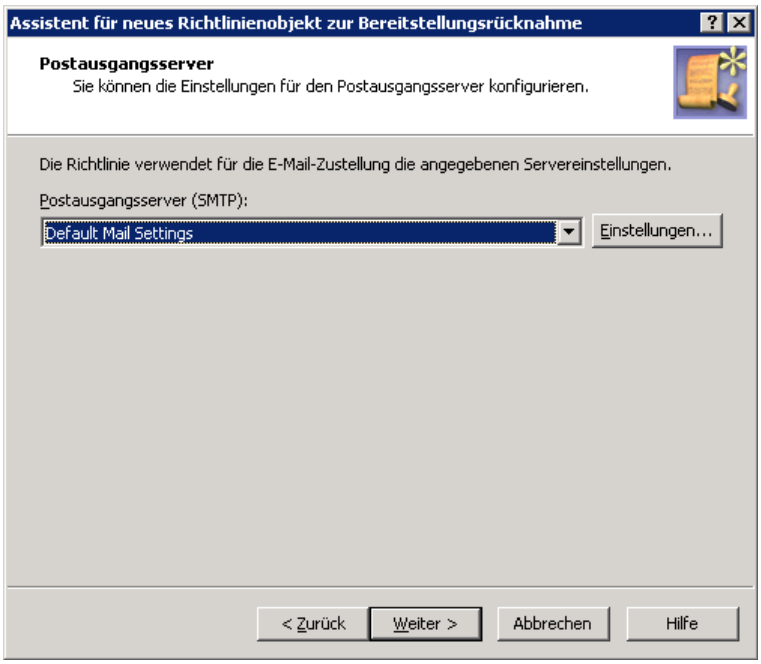
Auf dieser Seite können Sie eine Liste von Benachrichtigungsempfängern einrichten und ggf. alle notwendigen Änderungen am Betreff und Text der Nachricht vornehmen.

Klicken Sie zum Angeben von Benachrichtigungsempfängern auf die Schaltfläche neben dem Feld **Benachrichtigungsempfänger**, und geben Sie dann mindestens eine E-Mail-Adresse ein. Trennen Sie die Adressen der Benachrichtigungsempfänger mit Semikolons.

Wenn Sie die Benachrichtigungsmeldung ändern möchten, geben Sie Text in das Feld **Nachrichtenbetreff** oder **Nachrichtentext** ein. Sie können Makros verwenden, um Informationen zu dem zu deprovisionierenden Objekt einzugeben, damit die Nachricht für die Empfänger aussagekräftiger wird.

Makros haben dieselbe Syntax und Semantik wie Werte für Richtlinienbedingungen in Richtlinien zur Erzeugung und Validierung von Eigenschaften: Der LDAP-Anzeigename eines Attributs, eingeschlossen in spitze Klammern (<>) und mit einem Prozentzeichen (%) als Präfix, stellt den Wert dieses Attributs dar. Beispielsweise ersetzt ActiveRoles Server vor dem Senden einer Nachricht den Platzhalter %<name> durch den Namen des zu deprovisionierenden Objekts.

Klicken Sie nach Abschluss des Vorgangs auf **Weiter**, um die Seite **Postausgangsserver** anzuzeigen.



Auf dieser Seite können Sie die in der Richtlinie zu verwendende E-Mail-Konfiguration auswählen. Außerdem können Sie E-Mail-Einstellungen in der ausgewählten Konfiguration anzeigen oder ändern.

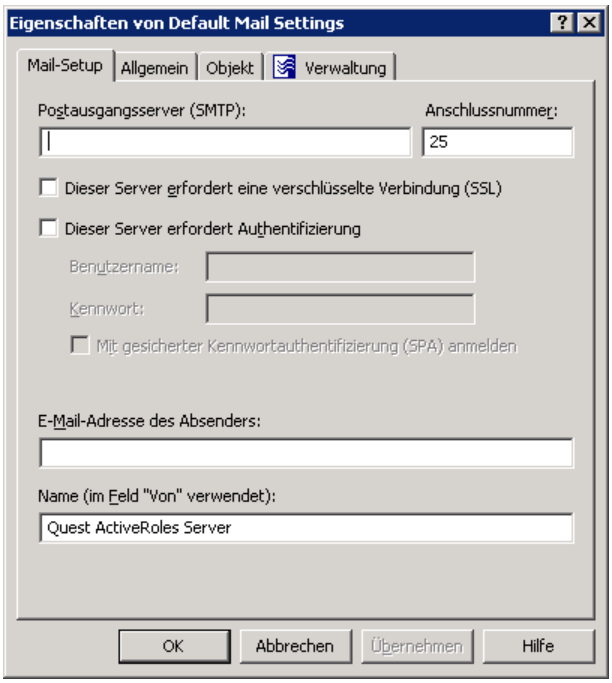
Wählen Sie zuerst in der Liste **Postausgangsserver (SMTP)** die E-Mail-Konfiguration aus, die von der Richtlinie verwendet werden soll.

Standardmäßig enthält die Liste **Postausgangsserver (SMTP)** einen einzelnen Eintrag. Mit der ActiveRoles Server-Konsole können Sie der Liste weitere Einträge hinzufügen. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration/Server Configuration**, klicken Sie mit der rechten Maustaste auf **Mail Configuration**, wählen Sie **Neu | Mail-Konfiguration** aus und folgen Sie dann den Anweisungen des Assistenten.

Jede E-Mail-Konfiguration gibt einen SMTP-Server an und stellt Informationen bereit, die zum Herstellen einer Verbindung mit diesem Server erforderlich sind. Um Konfigurationsparameter anzuzeigen und zu ändern, klicken Sie auf die Schaltfläche **Einstellungen**.

Konfigurieren von E-Mail-Einstellungen

Wenn Sie auf die Schaltfläche **Einstellungen** klicken, wird auf der Konsole das Dialogfeld **Eigenschaften** für die ausgewählte E-Mail-Konfiguration angezeigt. Dabei ähnelt die Registerkarte **Mail-Setup** der folgenden Abbildung.



Auf dieser Registerkarte können Sie die folgenden E-Mail-Einstellungen konfigurieren:

- **Postausgangsserver (SMTP)** Geben Sie die vollständig qualifizierte Adresse des zu verwendenden SMTP-Servers ein. Beispiel: smtp.mycompany.com.
- **Anschlussnummer** Geben Sie die Portnummer auf dem SMTP-Server an, über die die Verbindung hergestellt werden soll. Normalerweise ist auf dem SMTP-Server diese Portnummer auf 25 festgelegt.
- **Dieser Server erfordert eine verschlüsselte Verbindung (SSL)** Aktivieren Sie dieses Kontrollkästchen, wenn die Clients des SMTP-Servers beim Senden von Nachrichten über das Netzwerk SSL (Secure Sockets Layer) verwenden müssen.
- **Dieser Server erfordert Authentifizierung** Aktivieren Sie dieses Kontrollkästchen, wenn die Konfiguration des SMTP-Servers die Verwendung der Standardauthentifizierung oder der integrierten Windows-Authentifizierung vorsieht. Geben Sie dann den Benutzernamen und das Kennwort in die Felder unter dieser Option ein. ActiveRoles Server übergibt diese Rechtezuweisungen bei der Verbindungseinrichtung an den SMTP-Server.
- **Mit gesicherter Kennwortauthentifizierung (SPA) anmelden** Aktivieren Sie dieses Kontrollkästchen, wenn die Konfiguration des SMTP-Servers die Verwendung der integrierten Windows-Authentifizierung vorsieht, damit das Benutzerkennwort nicht über das Netzwerk übertragen wird.
- **E-Mail-Adresse des Absenders** Die standardmäßige E-Mail-Adresse des Nachrichten-absenders. Es muss eine gültige E-Mail-Adresse angegeben werden.
- **Name (im Feld „Von" verwendet)** Geben Sie den Standardnamen des Nachrichten-absenders an, der im Feld **Von** der mit dieser E-Mail-Konfiguration gesendeten Nachrichten angezeigt werden soll.

Klicken Sie nach dem Konfigurieren der Einstellungen für den E-Mail-Server auf **OK**, um das Dialogfeld **Eigenschaften** für die E-Mail-Konfiguration zu schließen. Klicken Sie dann auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schrittweise Anleitungen finden Sie unter **Anleitungen/Verwalten von Richtlinienobjekten/ Konfigurieren von Deprovisionsrichtlinienobjekten/Konfigurieren einer Richtlinie zur Verbreitung von Benachrichtigungen** in der ActiveRoles Server-Hilfe.

Szenario: Senden einer Deprovisionierungsbenachrichtigung an den Administrator

In diesem Szenario wird das Konfigurieren einer Richtlinie beschrieben, mit der der Administrator benachrichtigt wird, wenn Objekte in einer beliebigen bei ActiveRoles Server registrierten Domäne (verwalteten Domäne) deprovisioniert werden.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen Sie die entsprechende E-Mail-Konfiguration.
2. Erstellen und konfigurieren Sie das Richtlinienobjekt, das die entsprechende Richtlinie definiert, und wenden Sie es an.

Folglich wird der Administrator bei einer Deprovisionsanforderung für ein Objekt wie etwa ein Benutzer oder eine Gruppe in einer beliebigen verwalteten Domäne mit Hilfe einer E-Mail-Nachricht über die Anforderung informiert. Die Nachricht umfasst den Namen des zu deprovisionierenden Objekts.

In den folgenden beiden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen der E-Mail-Konfiguration

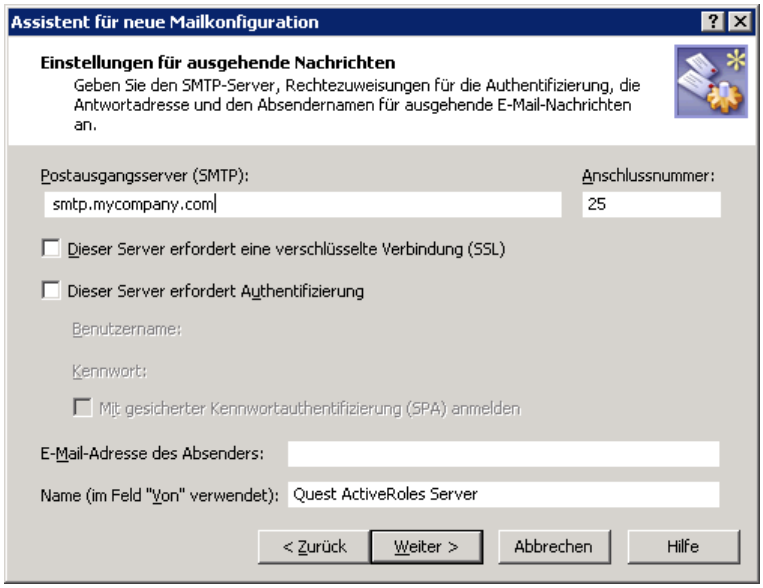
In diesem Szenario wird Folgendes für Ihren SMTP-Server vorausgesetzt:

- Er wird auf dem Server **smtp.mycompany.com** ausgeführt
- Verwendet die **Standard-Portnummer (25)**
- Er lässt den **anonymen Zugriff** zu
- Er lässt **nicht verschlüsselte Verbindungen** zu

Erstellen Sie die E-Mail-Konfiguration wie folgt mit Hilfe der ActiveRoles Server-Konsole:

1. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration | Server configuration**, klicken Sie mit der rechten Maustaste auf **Mail Configuration** und wählen Sie dann **Neu | Mail-Konfiguration**, um den Assistenten „Neue E-Mail-Konfiguration" zu starten.
2. Klicken Sie auf **Weiter**.
3. Geben Sie unter **Name** den Wert **Verbreitung der Deprovisionierungsbenachrichtigung** ein.
4. Klicken Sie auf **Weiter**.

5. Geben Sie unter **Postausgangsserver (SMTP)** den Wert **smtp.mycompany.com** ein.
   Nach der Ausführung dieser Schritte sollte die Seite des Assistenten der folgenden Abbildung entsprechen.



6. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

Schritt 2: Erstellen, Konfigurieren und Anwenden des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt mit dem Assistenten „Neues Deprovisionsrichtlinienobjekt" erstellen, konfigurieren und anwenden. Weitere Informationen über den Assistenten finden Sie unter „Erstellen eines Richtlinienobjekts" im Abschnitt „Verwaltungsaufgaben für Richtlinienobjekte" weiter oben in diesem Kapitel.

Klicken Sie zum Konfigurieren der Richtlinie auf der Seite **Richtlinientyp auswählen** des Assistenten auf **Benachrichtigungsverteilung**. Klicken Sie dann auf **Weiter**.

Klicken Sie auf der Seite **Empfänger und Nachricht der Benachrichtigung** auf die Schaltfläche neben dem Feld **Benachrichtigungsempfänger**, um das Dialogfeld **Empfänger der Benachrichtigung zur Deprovisionierung** anzuzeigen. Geben Sie in diesem Dialogfeld die E-Mail-Adresse des Administrators ein (z.B. administrator@mydomain.com), und klicken Sie dann auf **OK**.

Passen Sie dann den Betreff und den Text der Nachricht wie gewünscht an. Sie können beispielsweise den folgenden Betreff und Text eingeben:

Betreff der Nachricht

Deprovisionierung von %<Objektklasse> '%<Name>' angefordert

Text der Nachricht

Deprovisionierung von %<Objektklasse> '%<Name>' wird ausgeführt:Führen Sie bei Bedarf weitere Deprovisionsvorgänge durch, um die Deprovisionierung für diese %<Objektklasse> abzuschließen.

Diese Benachrichtigung wurde von ActiveRoles Server gemäß unternehmensweiten Richtlinien zur Deprovisionierung automatisch erzeugt.

Klicken Sie auf **Weiter**, damit die Seite **Postausgangsserver** angezeigt wird.

Wählen Sie in der Liste im Feld **Postausgangsserver (SMTP)** den Eintrag **Verbreitung der Deprovisionierungsbenachrichtigung** aus. Dabei handelt es sich um die E-Mail-Konfiguration, die Sie in Schritt 1 erstellt haben. Klicken Sie dann auf **Weiter**, damit die Seite **Richtlinie erzwingen** angezeigt wird.

Fügen Sie der Liste auf der Seite **Richtlinie erzwingen** den Ordner **Active Directory** wie folgt hinzu:

1. Klicken Sie auf die Schaltfläche **Hinzufügen**, um das Fenster **Objekte auswählen** anzuzeigen.
2. Klicken Sie im Fenster **Objekte auswählen** auf die Schaltfläche **Durchsuchen**, um das Dialogfeld **Container suchen** anzuzeigen.
3. Klicken Sie im Dialogfeld **Container suchen** auf **Active Directory** und klicken Sie dann auf **OK**.
4. Wählen Sie in der oberen Liste im Fenster **Objekte auswählen** den Eintrag **Active Directory** aus.
5. Klicken Sie auf **Hinzufügen** und dann auf **OK**, um das Fenster **Objekte auswählen** zu schließen.

Klicken Sie auf **Weiter**, und klicken Sie dann auf **Fertig stellen**, um den Assistenten zu schließen.

Sie können auch in der Konsolenstruktur für den Ordner **Active Directory** den Befehl **Richtlinie erzwingen** verwenden, um die Richtlinie auf diesen Ordner anzuwenden. Weitere Informationen über die Anwendung eines Richtlinienobjekts finden Sie unter „Anwenden von Richtlinienobjekten“ und „Verwalten des Richtlinienbereichs“ weiter oben in diesem Kapitel.

Berichtsverteilung

Mit Richtlinien dieser Kategorie wird automatisch ein Bericht versendet, nachdem ein Deprovisions-vorgang abgeschlossen ist. Der Bericht enthält die Vorgangsergebnisse. Der primäre Zweck einer solchen Richtlinie ist es, bei Problemen während der Verarbeitung von Rücknahmeanforderungen ausgewählte Personen zu informieren. Diese Berichte werden weiter unten in diesem Kapitel beschrieben (siehe Abschnitt „Bericht zu Ergebnissen der Deprovision“).

Die Berichte werden per E-Mail übermittelt. Beim Konfigurieren der Richtlinie „Berichtsverteiler“ können Sie eine Liste von Berichtsempfängern einrichten, den Betreff der Berichtsnachrichten anpassen sowie angeben, ob bei Auftreten eines Fehlers ein Bericht gesendet werden soll oder nicht.

Funktionsweise dieser Richtlinie

Nach Abschluss eines Deprovisionsvorgangs ermittelt ActiveRoles Server anhand dieser Richtlinie, ob der Bericht mit den Ergebnissen der Deprovision versendet werden muss. Dann generiert ActiveRoles Server die Berichtsnachricht und versendet sie an die Empfänger, die in der Richtlinienkonfiguration angegeben sind. Der Bericht schließt eine Liste der Aktionen ein, die während des Deprovisionsvorgangs ausgeführt wurden. Für jede Aktion gibt der Bericht an, ob sie erfolgreich abgeschlossen wurde, und stellt Informationen zu ihren Ergebnissen bereit.

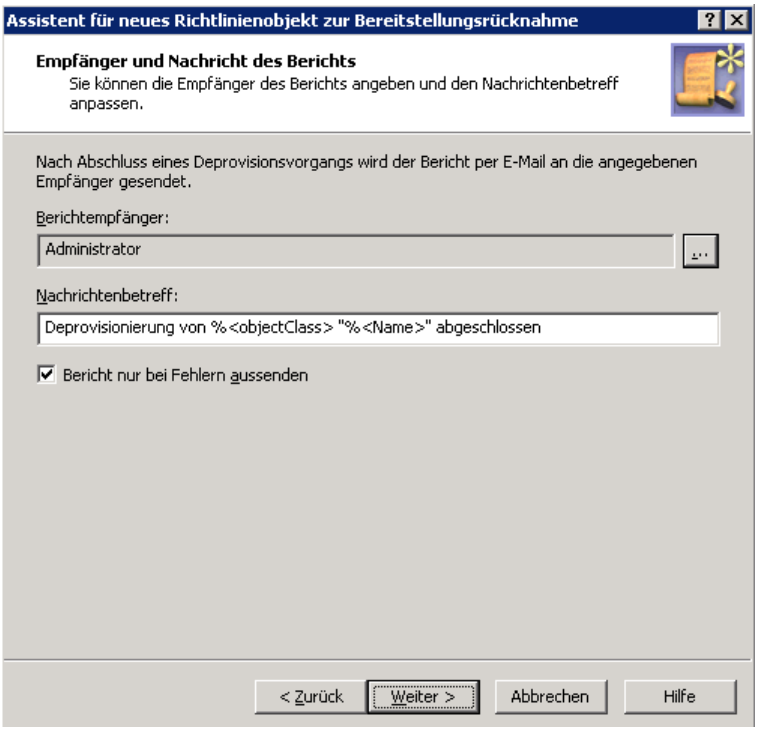
Wenn die Berichtsverteilungsrichtlinie so konfiguriert ist, dass keine Berichte gesendet werden, wenn keine Fehler aufgetreten sind, untersucht ActiveRoles Server die Deprovisionsergebnisse auf Fehler. Falls keine Fehler aufgetreten sind, wird der Bericht nicht versendet.

ActiveRoles Server generiert Berichte zur Deprovision pro Objekt: Jede Berichtsnachricht enthält Informationen zur Deprovision genau eines Objekts. Bei der Deprovision mehrerer Objekte versendet ActiveRoles Server mehrere Berichtsnachrichten, eine pro deprovisioniertem Objekt.

ActiveRoles Server sendet Berichtsnachrichten über einen SMTP-Server. Die Richtlinienkonfiguration gibt den SMTP-Server für ausgehende Nachrichten mit Hilfe von ActiveRoles Server-E-Mail-Einstellungen an, die den Namen des SMTP-Servers sowie für die Verbindungsherstellung notwendige Informationen enthalten.

Konfigurieren der Richtlinie „Berichtsverteiler"

Um die Richtlinie „Berichtsverteiler" zu konfigurieren, wählen Sie **Berichtsverteiler** auf der Seite **Zu konfigurierende Richtlinie** im Assistenten „Neues Deprovisionsrichtlinienobjekt" oder im Assistenten „Deprovisionsrichtlinie hinzufügen" aus. Klicken Sie dann auf **Weiter**, damit die Seite **Empfänger und Nachricht des Berichts** angezeigt wird.


Assistent für neues Richtlinienobjekt zur Bereitstellungsrücknahme
Empfänger und Nachricht des Berichts
Sie können die Empfänger des Berichts angeben und den Nachrichtenbetreff anpassen.
Nach Abschluss eines Deprovisionsvorgangs wird der Bericht per E-Mail an die angegebenen Empfänger gesendet.
Berichtempfänger:
Administrator
...
Nachrichtenbetreff:
Deprovisionierung von %<objectClass> "%<Name>" abgeschlossen
Bericht nur bei Fehlern aussenden
< Zurück
Weiter >
Abbrechen
Hilfe

Auf dieser Seite können Sie eine Liste von Berichtsempfängern einrichten, ggf. alle notwendigen Änderungen am Betreff der Nachricht ändern sowie angeben, ob die Richtlinie den Bericht auch dann versenden soll, wenn während des Deprovisionsvorgangs keine Fehler aufgetreten sind.

Klicken Sie zum Angeben von Berichtsempfängern auf die Schaltfläche neben dem Feld **Berichtempfänger**, und geben Sie dann mindestens eine E-Mail-Adresse ein. Trennen Sie die Adressen der Benachrichtigungsempfänger mit Semikolons.

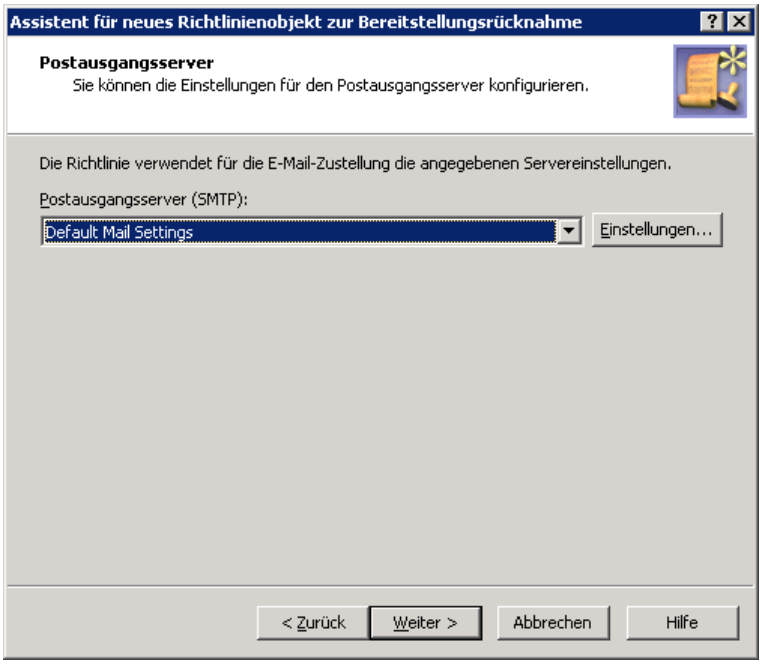
Wenn Sie den Betreff der Nachricht ändern möchten, geben Sie Text in das Feld **Nachrichtenbetreff** ein. Sie können Makros verwenden, um Informationen zu dem deprovisionierten Objekt einzugeben, damit die Nachricht für die Empfänger aussagekräftiger wird.

Makros haben dieselbe Syntax und Semantik wie Werte für Richtlinienbedingungen in Richtlinien zur Erzeugung und Validierung von Eigenschaften: Der LDAP-Anzeigename eines Attributs, eingeschlossen in spitze Klammern (<>) und mit einem Prozentzeichen (%) als Präfix, stellt den Wert dieses Attributs dar. Beispielsweise ersetzt ActiveRoles Server vor dem Senden einer Nachricht den Platzhalter %<name> durch den ursprünglichen Namen des deprovisionierten Objekts.

ActiveRoles Server ruft den Attributwert vor Beginn des Deprovisionsvorgangs ab, sodass der zu diesem Zeitpunkt aktuelle Wert vorliegt. Auch wenn eine Deprovisionsrichtlinie konfiguriert ist, die ein bestimmtes Attribut aktualisiert, wird für die Nachricht der ursprüngliche und nicht der aktualisierte Wert des Attributs gelesen.

Wenn die Richtlinie den Bericht unabhängig davon versenden soll, ob der Deprovisionsvorgang ohne Fehler abgeschlossen wurde, deaktivieren Sie das Kontrollkästchen **Bericht nur bei Fehlern aussenden**. andernfalls wird der Bericht nicht gesendet, wenn das Objekt ohne Fehler deprovisioniert wurde.

Klicken Sie nach Abschluss des Vorgangs auf **Weiter**, um die Seite **Postausgangsserver** anzuzeigen.



Diese Seite ähnelt der entsprechenden Assistentenseite zum Benachrichtigungsverteilung (siehe voriger Abschnitt). Sie können die in der Richtlinie zu verwendende E-Mail-Konfiguration auswählen. Außerdem können Sie E-Mail-Einstellungen in der ausgewählten Konfiguration anzeigen oder ändern.

Wählen Sie zuerst in der Liste **Postausgangsserver (SMTP)** die E-Mail-Konfiguration aus, die von der Richtlinie verwendet werden soll.

Standardmäßig enthält die Liste **Postausgangsserver (SMTP)** einen einzelnen Eintrag. Mit der ActiveRoles Server-Konsole können Sie der Liste weitere Einträge hinzufügen. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration/Server Configuration**, klicken Sie mit der rechten Maustaste auf **Mail Configuration**, wählen Sie **Neu | Mail-Konfiguration** aus, und folgen Sie dann den Anweisungen des Assistenten.

Jede E-Mail-Konfiguration gibt einen SMTP-Server an und stellt Informationen bereit, die zum Herstellen einer Verbindung mit diesem Server erforderlich sind. Um Konfigurationsparameter anzuzeigen und zu ändern, klicken Sie auf die Schaltfläche **Einstellungen**. Anweisungen finden Sie im Unterabschnitt „Konfigurieren der Richtlinie „Benachrichtigungsverteiler"" im vorigen Abschnitt.

Klicken Sie nach Abschluss des Vorgangs auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schrittweise Anleitungen finden Sie unter **Anleitungen/Verwalten von Richtlinienobjekten/ Konfigurieren von Deprovisionsrichtlinienobjekten/Konfigurieren einer Richtlinie zur Verbreitung von Berichten** in der ActiveRoles Server-Hilfe.

Szenario: Senden eines Deprovisionierungsberichts an den Administrator

In diesem Szenario wird beschrieben, wie Sie die folgende Richtlinie so konfigurieren, dass Deprovisionsvorgänge in allen bei ActiveRoles Server registrierten Domänen (verwalteten Domänen) überwacht werden:

- Überprüfen Sie nach Abschluss eines Deprovisionsvorgangs, ob während des Vorgangs Fehler aufgetreten sind.
- Wenn Fehler aufgetreten sind, wird der Bericht über die Deprovisionierungsergebnisse an den Administrator gesendet.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen Sie die entsprechende E-Mail-Konfiguration.
2. Erstellen und konfigurieren Sie das Richtlinienobjekt, das die entsprechende Richtlinie definiert, und wenden Sie es an.

Folglich erhält der Administrator nach Abschluss eines Deprovisionsvorgangs in einer beliebigen verwalteten Domäne einen Bericht, falls während des Vorgangs ein Fehler aufgetreten ist. Der Nachrichtenbetreff enthält den Namen des deprovisionierten Objekts.

In den folgenden beiden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen der E-Mail-Konfiguration

Sie können die im vorigen Abschnitt aufgeführten Anweisungen verwenden, um die E-Mail-Konfiguration zu erstellen (siehe „Szenario: Senden einer Deprovisionierungsbenachrichtigung an den Administrator"). Wenn Sie aufgefordert werden, einen Namen für die neuen Konfiguration einzugeben, geben Sie **Verbreitung des Deprovisionierungsberichts** ein.

Schritt 2: Erstellen, Konfigurieren und Anwenden des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt mit dem Assistenten „Neues Deprovisionsrichtlinienobjekt" erstellen, konfigurieren und anwenden. Weitere Informationen über den Assistenten finden Sie unter „Erstellen eines Richtlinienobjekts" im Abschnitt „Verwaltungsaufgaben für Richtlinienobjekte" weiter oben in diesem Kapitel.

Klicken Sie zum Konfigurieren der Richtlinie auf der Seite **Richtlinientyp auswählen** des Assistenten auf **Berichtsverteiler**. Klicken Sie dann auf **Weiter**.

Klicken Sie auf der Seite **Empfänger und Nachricht des Berichts** auf die Schaltfläche neben dem Feld **Berichtempfänger**, um das Dialogfeld **Empfänger des Deprovisionierungsberichts** anzuzeigen. Geben Sie in diesem Dialogfeld die E-Mail-Adresse des Administrators ein (z.B. administrator@mydomain.com), und klicken Sie dann auf **OK**.

Passen Sie dann den Betreff der Nachricht wie gewünscht an. Sie können beispielsweise den folgenden Betreff eingeben: *Deprovisionierung von %<Objektklasse> '%<Name>' Abgeschlossen mit Fehlern*. Klicken Sie auf **Weiter**, damit die Seite **Postausgangsserver** angezeigt wird.

Wählen Sie in der Liste im Feld **Postausgangsserver (SMTP)** den Eintrag **Verbreitung des Deprovisionierungsberichts** aus. Dabei handelt es sich um die E-Mail-Konfiguration, die Sie in Schritt 1 erstellt haben. Stellen Sie sicher, dass das Kontrollkästchen **Bericht nur bei Fehlern aussenden** aktiviert ist, und klicken Sie dann auf **Weiter**, um die Seite **Richtlinie erzwingen** anzuzeigen.

Klicken Sie auf der Seite **Richtlinie erzwingen** auf die Schaltfläche **Hinzufügen**, und wählen Sie den Ordner **Active Directory** aus, um ihn der Liste hinzuzufügen. Eine detaillierte Anleitung finden Sie im vorigen Abschnitt (siehe „Szenario: Senden einer Deprovisionierungsbenachrichtigung an den Administrator"). Klicken Sie auf **Weiter**, und klicken Sie dann auf **Fertig stellen**, um den Assistenten zu schließen.

Sie können auch in der Konsolenstruktur für den Ordner **Active Directory** den Befehl **Richtlinie erzwingen** verwenden, um die Richtlinie auf diesen Ordner anzuwenden. Weitere Informationen über die Anwendung eines Richtlinienobjekts finden Sie unter „Anwenden von Richtlinienobjekten" und „Verwalten des Richtlinienbereichs" weiter oben in diesem Kapitel.

Überprüfen der Richtlinieneinhaltung

Beim Überprüfen auf Richtlinieneinhaltung werden Informationen zu Verzeichnisdaten bereitgestellt, die den mit ActiveRoles Server definierten Richtlinien nicht entsprechen, z.B. Namenskonventionen für Benutzer oder Gruppen. Wenn Sie Richtlinien definieren, nachdem bereits Daten eingegeben wurden, können Sie die Daten überprüfen und sie entsprechend ändern, um sicherzustellen, dass sie die Richtlinienanforderungen erfüllen.

Zwar können mit ActiveRoles Server Geschäftsregeln und Richtlinien normalerweise nicht mehr umgangen werden, nachdem sie konfiguriert sind; es gibt jedoch Situationen, in denen die tatsächlichen Verzeichnisdaten möglicherweise einige der vorgeschriebenen Richtlinien oder Geschäftsregeln verletzen. Beispielsweise überprüft ActiveRoles Server beim Anwenden einer neuen Richtlinie nicht automatisch die vorhandenen Verzeichnisdaten, um zu ermitteln, ob sie der neuen Richtlinie entsprechen. Ein weiteres Beispiel ist ein Prozess, der automatisch neue Objekte wie etwa Benutzer- oder Gruppenobjekte erstellt, indem er direkt auf Active Directory zugreift und ActiveRoles Server nicht verwendet.

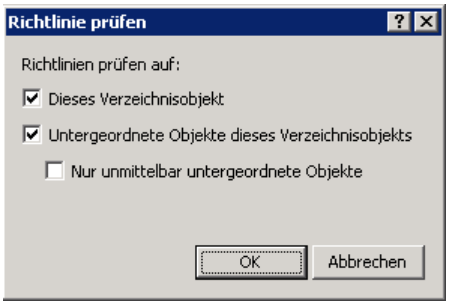
Das Berichterstattungspaket von ActiveRoles Server enthält eine Reihe von Berichten, die bei der Erkennung von Richtlinienübertretungen in Verzeichnisdaten helfen, indem sie Informationen zum Zustand der Verzeichnisobjekte im Verhältnis zu den vorgeschriebenen Richtlinien sammeln und analysieren. Da das Abrufen derartiger Informationen jedoch zeitintensiv und aufwändig sein kann, ermöglichen die Berichte zur Richtlinieneinhaltung es manchmal nicht, richtlinienbezogene Probleme zeitnah zu lösen.

Um diesem Problem zu begegnen, ermöglicht ActiveRoles Server die schnelle Erstellung und Untersuchung von Richtlinienüberprüfungsergebnissen für einzelne Objekte oder gesamte Container. Die Richtlinienüberprüfungsergebnisse stellen eine Liste von Verzeichnisobjekten bereit, die Richtlinien verletzen, und beschreiben die erkannten Verletzungen. Anhand der Richtlinienüberprüfungsergebnisse können Sie geeignete Änderungen an Objekten oder Richtlinien vornehmen:

- Ändern von Objekteigenschaften in Übereinstimmung mit Richtlinien.
- Verhindern der Auswirkung bestimmter Richtlinien auf einzelne Objekte.
- Ändern von Richtlinienobjekten nach Bedarf.
- Ausführen einer Verwaltungsaufgabe, z.B. Deaktivieren oder Verschieben von Benutzerobjekten, die Regeln verletzen.

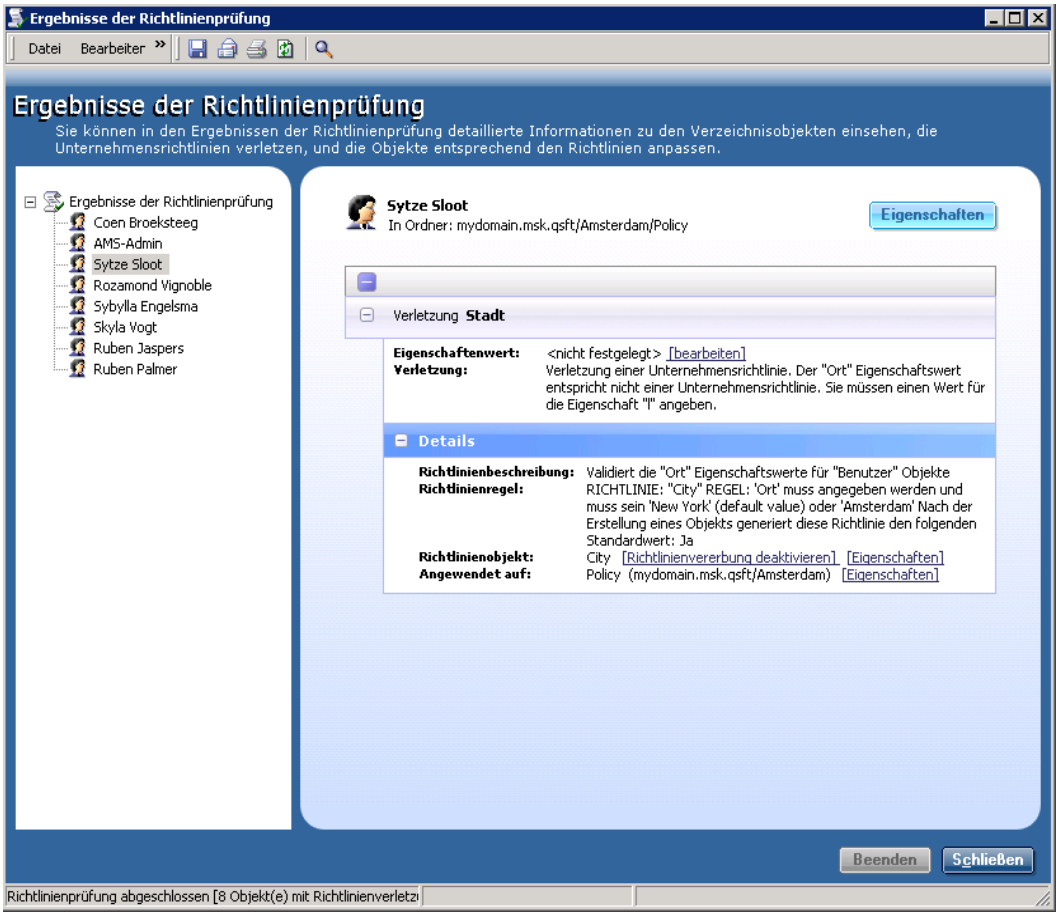
Zusätzlich können Sie Richtlinienüberprüfungsergebnisse in einer Datei speichern, drucken oder an einen E-Mail-Empfänger senden.

Um die Richtlinieneinhaltung eines Objekts zu überprüfen, klicken Sie mit der rechten Maustaste auf das Objekt und klicken dann auf **Richtlinie prüfen**. Bei einem Containerobjekt wird nun das Dialogfeld **Richtlinie prüfen** angezeigt, das in der folgenden Abbildung gezeigt wird.



Aktivieren Sie im Dialogfeld **Richtlinie prüfen** die entsprechenden Kontrollkästchen, um den Bereich des Vorgangs anzugeben, und klicken dann auf **OK**.

Das Fenster **Ergebnisse der Richtlinienprüfung** wird angezeigt, und der Vorgang wird gestartet. Die Überprüfungsergebnisse werden im rechten Bereich des Fensters angezeigt (siehe Abbildung unten).


Ergebnisse der Richtlinienprüfung
Datei
Bearbeiter
Ergebnisse der Richtlinienprüfung
Sie können in den Ergebnissen der Richtlinienprüfung detaillierte Informationen zu den Verzeichnisobjekten einsehen, die Unternehmensrichtlinien verletzen, und die Objekte entsprechend den Richtlinien anpassen.
Ergebnisse der Richtlinienprüfung
Coen Broeksteeg
AMS-Admin
Sytze Sloot
Rozamond Vignoble
Sybylla Engelsma
Skyla Vogt
Ruben Jaspers
Ruben Palmer
Sytze Sloot
In Ordner: mydomain.msk.qsft/Amsterdam/Policy
Eigenschaften
Verletzung Stadt
Eigenschaftenwert: <nicht festgelegt> [bearbeiten]
Verletzung: Verletzung einer Unternehmensrichtlinie. Der "Ort" Eigenschaftswert entspricht nicht einer Unternehmensrichtlinie. Sie müssen einen Wert für die Eigenschaft "l" angeben.
Details
Richtlinienbeschreibung: Validiert die "Ort" Eigenschaftswerte für "Benutzer" Objekte
Richtlinienregel: RICHTLINIE: "City" REGEL: 'Ort' muss angegeben werden und muss sein 'New York' (default value) oder 'Amsterdam' Nach der Erstellung eines Objekts generiert diese Richtlinie den folgenden Standardwert: Ja
Richtlinienobjekt: City [Richtlinienvererbung deaktivieren] [Eigenschaften]
Angewendet auf: Policy (mydomain.msk.qsft/Amsterdam) [Eigenschaften]
Beenden
Schließen
Richtlinienprüfung abgeschlossen [8 Objekt(e) mit Richtlinienverletzu

Die Objekte, die eine Richtlinie verletzen, werden im linken Bereich angezeigt. Wenn Sie im linken Bereich auf ein Objekt klicken, wird die Richtlinienverletzung im rechten Bereich detailliert beschrieben.

Standardmäßig werden im rechten Bereich des Fensters **Ergebnisse der Richtlinienprüfung** nur grundlegende Optionen angezeigt. Sie können mehrere Optionen anzeigen, indem Sie auf die Spaltenüberschrift der Spalte **Details** klicken.

Mit Hilfe der Verknüpfungen im linken Bereich können Sie folgende Aufgaben ausführen:

- Ändern des Eigenschaftswerts, der die Richtlinie verletzt: Klicken Sie auf die Verknüpfung **Bearbeiten** neben der Beschriftung **Eigenschaftenwert**.
- Entfernen des Objekts aus dem Bereich der Richtlinie: Klicken Sie auf die Verknüpfung **Richtlinienvererbung deaktivieren** neben der Beschriftung **Richtlinienobjekt**. Dann steuert die Richtlinie das Objekt nicht mehr.
- Ändern der Richtlinie: Klicken Sie auf die Verknüpfung **Eigenschaften** neben der Beschriftung **Richtlinienobjekt**. Dies zeigt das Dialogfeld **Eigenschaften** für das Richtlinienobjekt an, das unter „Hinzufügen, Ändern und Entfernen von Richtlinien" weiter oben in diesem Kapitel beschrieben ist.

- Verwalten des Objekts, das die Richtlinie verletzt: Klicken Sie oben rechts im rechten Bereich auf die Schaltfläche **Eigenschaften**.
- Verwalten des Objekts, auf das das Richtlinienobjekt angewendet wird: Klicken Sie auf die Verknüpfung **Eigenschaften** neben der Beschriftung **Angewendet auf**.

Sie können sich anhand der folgenden Anweisungen mit dem Überprüfen der Richtlinieneinhaltung über die ActiveRoles Server-Konsole vertraut machen:

1. Erstellen und konfigurieren Sie ein Richtlinienobjekt mit der Richtlinie für die Generierung und Validierung von Eigenschaften für die Eigenschaft **Abteilung** von Benutzerobjekten. Geben Sie dabei die Richtlinienregel wie folgt an: *Wert muss angegeben werden und muss „Sales" oder „Production" lauten*.
2. Wenden Sie dieses Richtlinienobjekt auf eine Organisationseinheit an, die bereits Benutzerobjekte ohne Angabe der Abteilung enthält (verknüpfen Sie es mit ihr).
3. Klicken Sie mit der rechten Maustaste auf die Organisationseinheit und klicken Sie dann auf **Richtlinie prüfen**. Klicken Sie im Dialogfeld **Richtlinie prüfen** auf **OK**.

   *Nachdem Sie diese Schritte ausgeführt haben, wird das Fenster **Ergebnisse der Richtlinienprüfung** angezeigt. In seinem linken Bereich sind Objekte aufgelistet, die die Richtlinie verletzen.*
4. Warten Sie, während die Liste im linken Bereich aufgefüllt wird. Wählen Sie dann in der Liste ein Benutzerobjekt aus.

   *Im rechten Bereich neben der Bezeichnung **Verletzung** wird die Eingabeaufforderung „Sie müssen einen Wert für die Eigenschaft 'Abteilung' angeben" angezeigt.*
5. Klicken Sie im rechten Bereich auf die Verknüpfung **Bearbeiten** neben der Bezeichnung **Eigenschaftenwert**.
6. Wählen Sie im Dialogfeld **Eigenschaften** im Kombinationsfeld **Abteilung** einen der zulässigen Werte (**Production** oder **Sales**) aus.

Schrittweise Anleitungen bezüglich der Überprüfung von Objekten auf Richtlinienkonformität finden Sie unter **Anleitungen/Verwalten von Richtlinienobjekten/Überprüfen auf Richtlinienkonformität** in der ActiveRoles Server-Hilfe.

Deprovisionieren von Benutzern oder Gruppen

Die ActiveRoles Server-Konsole und das Web-Interface stellen den Befehl **Deprovision** für Benutzer- und Gruppenobjekte bereit. Dieser Befehl generiert eine Deprovisionsanforderung für die ausgewählten Objekte. Beim Verarbeiten der Anforderung führt ActiveRoles Server alle Vorgänge aus, die von den Deprovisionsrichtlinien vorgeschrieben werden.

Standardoptionen für die Deprovision

ActiveRoles Server enthält standardmäßig zwei integrierte Richtlinienobjekte, die die Vorgänge angeben, die bei der Deprovision eines Benutzers oder einer Gruppe ausgeführt werden sollen. Diese Richtlinienobjekte finden Sie in der ActiveRoles Server-Konsole, indem Sie den Container **Configuration | Policies | Administration | Builtin** auswählen.

Das Richtlinienobjekt **Built-in Policy – User Default Deprovisioning** legt die standardmäßigen Auswirkungen des Befehls **Deprovision** auf Benutzerkonten fest; das Richtlinienobjekt **Built-in Policy – Group Default Deprovisioning** legt die standardmäßigen Auswirkungen dieses Befehls auf Gruppen fest. Beide Objekte werden auf den Container **Active Directory** angewandt und wirken sich daher auf alle Domänen aus, die bei ActiveRoles Server registriert sind.

Die folgenden Tabellen fassen die Optionen der Standard-Deprovisionierungsrichtlinie zusammen. Wenn Sie die Deprovisionsrichtlinien nicht hinzufügen, entfernen oder ändern, führt ActiveRoles Server den Befehl **Deprovision** für einen Benutzer oder eine Gruppe anhand dieser Optionen aus.

Standard-Deprovisionierungsrichtlinienoptionsen für Benutzer, definiert durch das Richtlinienobjekt **Built-in Policy – User Default Deprovisioning**:

RICHTLINIE	OPTIONEN
Benutzerkonto-deprovisionierung	• Deaktivieren des Benutzerkontos • Festlegen des Kennworts des Benutzers auf einen zufälligen Wert • Ändern des Benutzernamens, sodass er das Deprovisionierungssuffix und das Datum der Deprovision dieses Benutzers enthält • Ausfüllen der Benutzerbeschreibung, um anzuzeigen, dass dieses Benutzerkonto deprovisioniert wurde • Löschen bestimmter Eigenschaften des Benutzerkontos, wie Stadt, Firma und Adresse
Entfernen der Gruppen-mitgliedschaft	• Entfernen des Benutzerkontos aus allen Sicherheitsgruppen • Entfernen des Benutzerkontos aus allen Verteilergruppen
Deprovisionierung des Exchange-Postfachs	• Benutzerpostfach in der Exchange-Adressliste ausblenden, um so den Zugriff auf das Postfach zu verhindern
Stammordner-Deprovisionierung	• Aufheben des Zugriffs auf den Benutzerstammordner über das Benutzerkonto • Gewähren von Lesezugriff auf den Stammordner des Benutzers an den Vorgesetzten des Benutzers • Festlegen der Administratorengruppe als Besitzer des Stammordners
Benutzerkonto-Verschiebung	• Belassen des Benutzerkontos in der Organisationseinheit, in der es sich zum Zeitpunkt der Deprovision befand
Permanentes Löschen von Benutzerkonten	• Verhindern der Löschung des Benutzerkontos

Standard-Deprovisionierungsrichtlinienoptionsen für Gruppen, definiert durch das Richtlinienobjekt **Built-in Policy – Group Default Deprovisioning**:

RICHTLINIE	OPTIONEN
Gruppenobjekt-Deprovisionierung	• Gruppentyp von „Sicherheit" in „Verteilung" ändern • Gruppe in der globalen Adressliste (GAL) ausblenden • Ändern des Gruppennamens, sodass er das Deprovisionierungssuffix und das Datum der Deprovision dieser Gruppe enthält • Alle Mitglieder aus der Gruppe entfernen • Ausfüllen der Gruppenbeschreibung, um anzuzeigen, dass diese Gruppe deprovisioniert wurde • Deaktivieren bestimmter Eigenschaften der Gruppe, um die Veröffentlichung der Gruppe in Self-Service Manager zu stoppen
Gruppenobjekt-Verschiebung	• Belassen der Gruppe in der Organisationseinheit, in der sie sich zum Zeitpunkt der Deprovision befand
Dauerhaftes Löschen des Gruppenobjekts	• Verhindern der Löschung der Gruppe

Delegieren der Deprovisionsaufgabe

Das Recht zur Deprovision besitzt standardmäßig das Administratorkonto „AR Server Admin", das während der Installation von ActiveRoles Server angegeben wird. Die Deprovisionierungsaufgabe kann jedoch an jeden beliebigen Benutzer und an jede beliebige Gruppe delegiert werden. Es wird eine ausschließlich für diesen Zweck vorgesehene Zugriffsvorlage bereitgestellt, damit Sie die Verwendung des Befehls **Deprovision** delegieren können, ohne zugleich die Rechte für den Erstellungs- oder Löschvorgang zu delegieren.

Um die Deprovision für Benutzer oder Gruppen in einem bestimmten Container (z.B. in einer Organisationseinheit oder einer verwalteten Einheit) zu delegieren, wenden Sie die Zugriffsvorlage wie folgt an:

Gehen Sie folgendermaßen vor, um die Deprovisionsaufgabe zu delegieren:

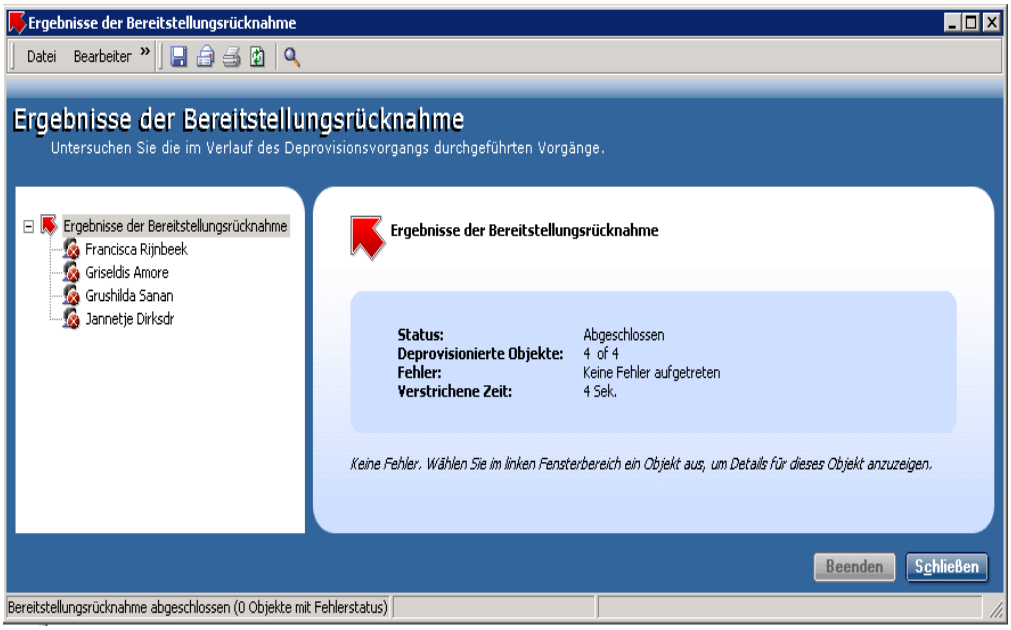
1. Klicken Sie in der ActiveRoles Server-Konsole mit der rechten Maustaste auf den Container und klicken Sie dann auf **Kontrolle delegieren**, um das Fenster **ActiveRoles Server-Sicherheit** anzuzeigen.
2. Klicken Sie im Fenster **ActiveRoles Server-Sicherheit** auf **Hinzufügen**, um den Assistenten „Delegation der Kontrolle" zu starten. Klicken Sie auf **Weiter**.
3. Klicken Sie auf der Seite **Benutzer oder Gruppen** auf **Hinzufügen**, und wählen Sie dann die Benutzer oder Gruppen aus, an die Sie die Rechte für Deprovisionsaufgabe delegieren möchten. Klicken Sie auf **Weiter**.
4. Erweitern Sie auf der Seite **Zugriffsvorlagen** den Ordner **Active Directory** und gehen Sie dann wie folgt vor:
   - Um die Aufgabe der Deprovisionierung von Benutzern zu delegieren, aktivieren Sie das Kontrollkästchen neben **Users – Perform Deprovision Tasks**.
   - Um die Aufgabe der Deprovisionierung von Gruppen zu delegieren, aktivieren Sie das Kontrollkästchen neben **Groups – Perform Deprovision Tasks**.
5. Klicken Sie auf **Weiter** und befolgen Sie die Anweisungen im Assistenten; übernehmen Sie bei diesem Vorgang die Standardeinstellungen.

Nachdem Sie diese Schritte abgeschlossen haben, sind die in Schritt 3 ausgewählten Benutzer und Gruppen autorisiert, Benutzer und Gruppen in dem in Schritt 1 ausgewählten Container und ggf. in allen seinen Untercontainern zu deprovisionieren.

Verwenden des Deprovisionsbefehls

Der Befehl **Deprovision** ist in der ActiveRoles Server-Konsole und im Web-Interface verfügbar. Mit dem Befehl **Deprovision** starten Sie den Deprovisionsvorgang für die ausgewählten Objekte.

Der Fortschritt und die Ergebnisse des Vorgangs werden im Fenster **Ergebnisse der Bereitstellungsrücknahme** angezeigt. Nach Abschluss des Vorgangs wird in dem Fenster die Vorgangszusammenfassung angezeigt, sodass Sie die Vorgangsergebnisse detailliert untersuchen können. Die folgende Abbildung zeigt eine typische Vorgangszusammenfassung.



Im linken Bereich werden die deprovisionierten Objekte aufgelistet. Im rechten Bereich werden der Vorgangsstatus und ggf. die Fehlermeldungen angezeigt.

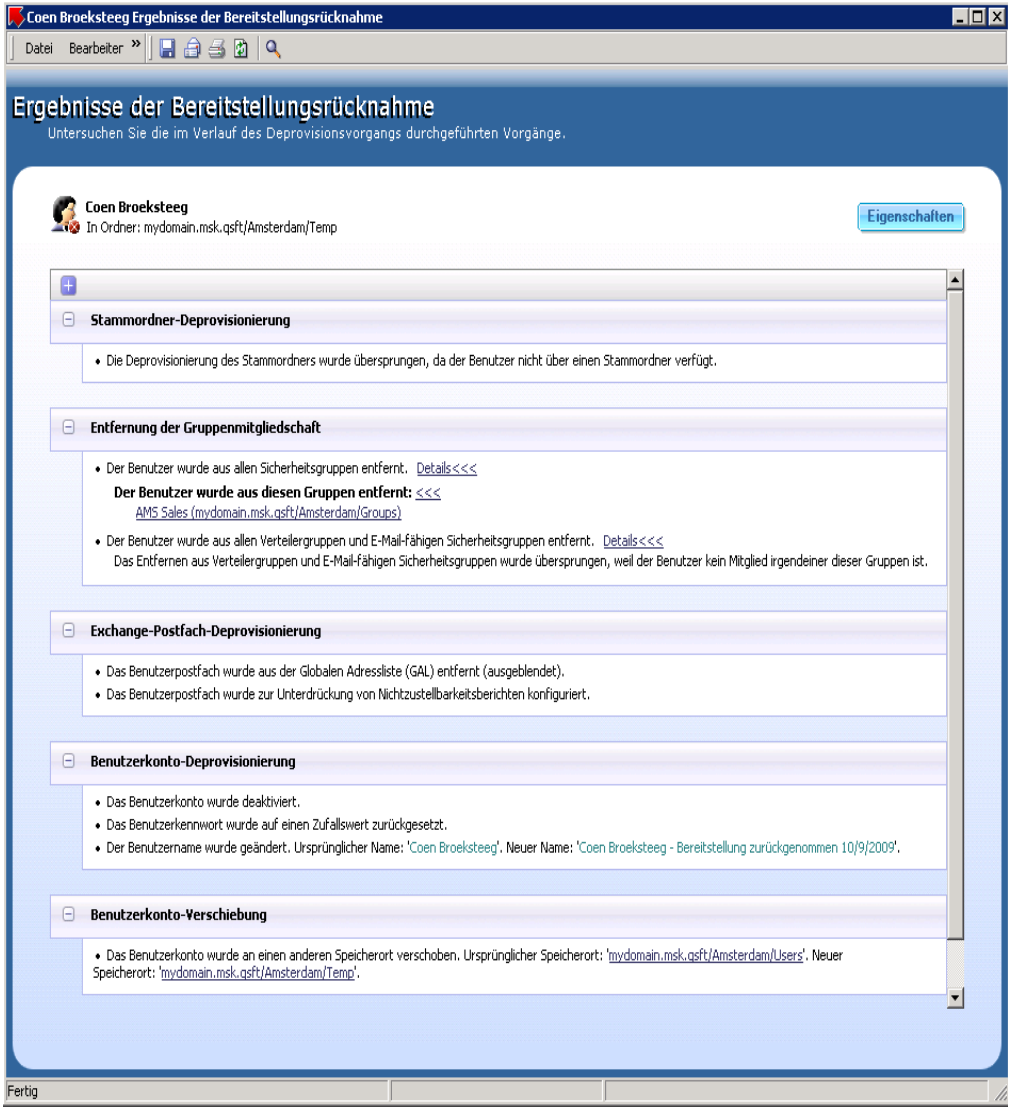
Um Vorgangsergebnisse anzuzeigen, wählen Sie im linken Bereich ein Objekt aus. Der rechte Bereich zeigt einen Bericht mit Informationen zu allen Aktionen, die während der Deprovision des ausgewählten Objekts ausgeführt wurden. Im nächsten Abschnitt wird ein beispielhafter Bericht erörtert.

Bericht zu Ergebnissen der Deprovision

Für jedes deprovisionierte Objekt können Sie im Fenster **Ergebnisse der Bereitstellungsrücknahme** die Ergebnisse des Deprovisionsvorgangs für dieses Objekt untersuchen.

Die ActiveRoles Server-Konsole oder das Web-Interface öffnet das Fenster **Ergebnisse der Bereitstellungsrücknahme**, wenn sie bzw. es den Befehl **Deprovision** ausführt. Sie können dieses Fenster auch mit Hilfe des Befehls **Ergebnisse der Bereitstellungsrücknahme** öffnen, der für deprovisionierte Objekte verfügbar ist.

Das Fenster **Ergebnisse der Bereitstellungsrücknahme** zeigt einen Bericht zum Deprovisionsvorgang an. Die folgende Abbildung zeigt einen typischen Bericht zu einem deprovisionierten Benutzerkonto:


Coen Broeksteeg Ergebnisse der Bereitstellungsrücknahme
Datei Bearbeiter
Ergebnisse der Bereitstellungsrücknahme
Untersuchen Sie die im Verlauf des Deprovisionsvorgangs durchgeführten Vorgänge.
Coen Broeksteeg
In Ordner: mydomain.msk.qsft/Amsterdam/Temp
Eigenschaften
Stammordner-Deprovisionierung
• Die Deprovisionierung des Stammordners wurde übersprungen, da der Benutzer nicht über einen Stammordner verfügt.
Entfernung der Gruppenmitgliedschaft
• Der Benutzer wurde aus allen Sicherheitsgruppen entfernt. Details<<<
Der Benutzer wurde aus diesen Gruppen entfernt: <<<
AMS Sales (mydomain.msk.qsft/Amsterdam/Groups)
• Der Benutzer wurde aus allen Verteilergruppen und E-Mail-fähigen Sicherheitsgruppen entfernt. Details<<<
Das Entfernen aus Verteilergruppen und E-Mail-fähigen Sicherheitsgruppen wurde übersprungen, weil der Benutzer kein Mitglied irgendeiner dieser Gruppen ist.
Exchange-Postfach-Deprovisionierung
• Das Benutzerpostfach wurde aus der Globalen Adressliste (GAL) entfernt (ausgeblendet).
• Das Benutzerpostfach wurde zur Unterdrückung von Nichtzustellbarkeitsberichten konfiguriert.
Benutzerkonto-Deprovisionierung
• Das Benutzerkonto wurde deaktiviert.
• Das Benutzerkennwort wurde auf einen Zufallswert zurückgesetzt.
• Der Benutzername wurde geändert. Ursprünglicher Name: 'Coen Broeksteeg'. Neuer Name: 'Coen Broeksteeg - Bereitstellung zurückgenommen 10/9/2009'.
Benutzerkonto-Verschiebung
• Das Benutzerkonto wurde an einen anderen Speicherort verschoben. Ursprünglicher Speicherort: 'mydomain.msk.qsft/Amsterdam/Users'. Neuer Speicherort: 'mydomain.msk.qsft/Amsterdam/Temp'.
Fertig

In dem Bericht sind Vorgangsergebnisse in Abschnitte gegliedert, die nach Richtlinienkategorien benannt sind. Jeder Abschnitt enthält Berichtselemente, die zu einer bestimmten Richtlinienkategorie gehören. Wenn Sie oben im Bericht auf die Überschrift klicken, wird der Bericht vollständig erweitert, und alle Berichtselemente werden angezeigt. Sie können auch einzelne Abschnitte in dem Bericht erweitern oder ausblenden, indem Sie auf die Überschrift des jeweiligen Berichts klicken.

Für bestimmte Elemente steht im Bericht die Option zur Verfügung, die Ansicht weiter zu erweitern und zusätzliche Informationen anzuzeigen. Durch Anklicken der Option **Liste** wird eine Liste von Elementen (z.B. Benutzer- oder Gruppeneigenschaften) anzeigen, die an dem Vorgang beteiligt sind. Indem Sie auf die Option **Details** klicken, können Sie das Vorgangsergebnis detaillierter untersuchen.

Das Fenster **Ergebnisse der Bereitstellungsrücknahme** erfüllt auch einige häufige Berichterstattungsanforderungen, einschließlich der Möglichkeit, alle Vorgangsergebnisse zum Drucken oder Anzeigen in einer Datei zu dokumentieren. Mit dem Kontextmenü können Sie den Bericht in eine Datei im HTML- oder XML-Format exportieren, ihn drucken oder über E-Mail versenden.

Berichtsinhalt

In den folgenden Tabellen sind die möglichen Berichtselemente aufgelistet. Es ist eine Tabelle pro Berichtsabschnitt vorhanden. Die Elemente in den einzelnen Abschnitten beschreiben Ergebnisse von den Aktionen, die in Übereinstimmung mit der entsprechenden Deprovisionierungsrichtlinie ausgeführt wurden. Berichtselemente enthalten außerdem Informationen zum Erfolg oder Fehler jeder Aktion. Bei einem Fehler enthält das Berichtselement eine Fehlerbeschreibung.

Nicht alle aufgelisteten Elemente müssen notwendigerweise in einem Bericht enthalten sein. Ein tatsächlicher Bericht enthält nur die Berichtselemente, die den konfigurierten Richtlinienoptionen entsprechen. Wenn die Richtlinie beispielsweise nicht für das Deaktivieren von Benutzerkonten konfiguriert ist, schließt der Bericht das Element zu dieser Aktion nicht ein.

Berichtsabschnitt: Benutzerkontodeprovisionierung

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Das Benutzerkonto ist deaktiviert.	Das Benutzerkonto konnte nicht deaktiviert werden.
Das Benutzerkennwort wird auf einen Zufallswert zurückgesetzt.	Zurücksetzen des Benutzerkennworts fehlgeschlagen.
Der Benutzeranmeldename wird in einen Zufallswert geändert.	Der Benutzeranmeldename konnte nicht geändert werden.
Der Benutzeranmeldename (Prä-Windows 2000) wird in einen Zufallswert geändert.	Der Benutzeranmeldename (vor Windows 2000) konnte nicht geändert werden.
Der Benutzername wurde geändert. Originalname: *Name* Neuer Name: *Name*	Der Benutzername konnte nicht geändert werden. Aktueller Name: *Name* Der folgende Name konnte nicht festgelegt werden: *Name*
Die Benutzereigenschaften werden geändert. Liste: • *Benutzereigenschaften, alte und neue Eigenschaftswerte*	Die Benutzereigenschaften konnten nicht geändert werden. Liste: • *Benutzereigenschaften, Fehlerbeschreibung*

Berichtsabschnitt: Entfernen der Gruppenmitgliedschaft

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Der Benutzer wird in Übereinstimmung mit der Richtlinie nicht aus Sicherheitsgruppen entfernt (Ausnahme: dynamische Gruppen und von einer Gruppenfamilie kontrollierte Gruppen). Details: • *Sicherheitsgruppen, zu denen der Benutzer gehört*	*Nicht zutreffend*
Der Benutzer wird aus allen Sicherheitsgruppen entfernt. Details: • *Sicherheitsgruppen, aus denen der Benutzer entfernt wird*	Der Benutzer konnte aus einigen Sicherheitsgruppen nicht entfernt werden. Details: • *Sicherheitsgruppen, aus denen der Benutzer entfernt wird* • *Sicherheitsgruppen, aus denen der Benutzer aufgrund eines Fehlers nicht entfernt wird*
In Übereinstimmung mit der Richtlinie verbleibt der Benutzer in einigen Sicherheitsgruppen. Details: • *Sicherheitsgruppen, aus denen der Benutzer entfernt wird* • *Sicherheitsgruppen, aus denen der Benutzer in Übereinstimmung mit der Richtlinie nicht entfernt wird*	Der Benutzer konnte aus einigen Sicherheitsgruppen nicht entfernt werden. Details: • *Sicherheitsgruppen, aus denen der Benutzer entfernt wird* • *Sicherheitsgruppen, aus denen der Benutzer in Übereinstimmung mit der Richtlinie nicht entfernt wird* • *Sicherheitsgruppen, aus denen der Benutzer aufgrund eines Fehlers nicht entfernt wird*
Der Benutzer wird in Übereinstimmung mit der Richtlinie nicht aus Verteilergruppen oder E-Mail-fähigen Sicherheitsgruppen entfernt (Ausnahme: dynamische Gruppen und von einer Gruppenfamilie kontrollierte Gruppen). Details: • *Verteilergruppen und E-Mail-fähige Sicherheitsgruppen, zu denen der Benutzer gehört*	*Nicht zutreffend*
Der Benutzer wird aus allen Verteilergruppen und E-Mail-fähigen Sicherheitsgruppen entfernt. Details: • *Verteilergruppen und E-Mail-fähige Sicherheitsgruppen, aus denen der Benutzer entfernt wird*	Der Benutzer konnte aus einigen Verteilergruppen oder E-Mail-fähigen Sicherheitsgruppen nicht entfernt werden. Details: • *Verteilergruppen und E-Mail-fähige Sicherheitsgruppen, aus denen der Benutzer entfernt wird* • *Verteilergruppen oder E-Mail-fähige Sicherheitsgruppen, aus denen der Benutzer aufgrund eines Fehlers nicht entfernt wird*
In Übereinstimmung mit der Richtlinie verbleibt der Benutzer in einigen Verteilergruppen oder E-Mail-fähigen Sicherheitsgruppen. Details: • *Verteilergruppen und E-Mail-fähige Sicherheitsgruppen, aus denen der Benutzer entfernt wird* • *Verteilergruppen oder E-Mail-fähige Sicherheitsgruppen, aus denen der Benutzer in Übereinstimmung mit der Richtlinie nicht entfernt wird*	Der Benutzer konnte aus einigen Verteilergruppen oder E-Mail-fähigen Sicherheitsgruppen nicht entfernt werden. Details: • *Verteilergruppen und E-Mail-fähige Sicherheitsgruppen, aus denen der Benutzer entfernt wird* • *Verteilergruppen oder E-Mail-fähige Sicherheitsgruppen, aus denen der Benutzer in Übereinstimmung mit der Richtlinie nicht entfernt wird* • *Verteilergruppen oder E-Mail-fähige Sicherheitsgruppen, aus denen der Benutzer aufgrund eines Fehlers nicht entfernt wird*

Berichtsabschnitt: Deprovisionierung des Exchange-Postfachs

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Die Deprovisionierung des Postfachs wird übersprungen, da der Benutzer nicht über ein Exchange-Postfach verfügt.	*Nicht zutreffend*
Das Benutzerpostfach wird aus der Globalen Adressliste (GAL) entfernt (ausgeblendet).	Das Benutzerpostfach konnte nicht aus der Globalen Adressliste (GAL) entfernt (ausgeblendet) werden.
Das Benutzerpostfach wird zur Unterdrückung von Nichtzustellbarkeitsberichten konfiguriert.	Das Benutzerpostfach konnte nicht für die Unterdrückung von Nichtzustellbarkeitsberichten konfiguriert werden.
Dem Benutzerverwalter wird ein Vollzugriff auf das Benutzerpostfach gewährt. Name des Verwalters: *Name*	Dem Benutzerverwalter konnte kein Zugriff auf das Benutzerpostfach gewährt werden. Name des Verwalters: *Name*
Nicht zutreffend	Dem Benutzerverwalter konnte kein Zugriff auf das Benutzerpostfach gewährt werden. Grund: Der Benutzerverwalter ist nicht im Verzeichnis angegeben.
Den erforderlichen Benutzern und Gruppen wurde Vollzugriff auf das Benutzerpostfach gewährt. Liste: • *Benutzer und Gruppen*	Den erforderlichen Benutzern und Gruppen konnte kein Zugriff auf das Benutzerpostfach gewährt werden. Liste: • *Benutzer und Gruppen*
Die Weiterleitung von Nachrichten an alternative Empfänger ist für das Benutzerpostfach nicht zulässig.	Die Weiterleitung von Nachrichten an alternative Empfänger konnte für das Benutzerpostfach nicht verweigert werden.
Das Benutzerpostfach ist für die Weiterleitung eingehender Nachrichten an den Benutzerverwalter konfiguriert.	Das Benutzerpostfach konnte nicht für die Weiterleitung eingehender Nachrichten an den Benutzerverwalter konfiguriert werden.
Das Benutzerpostfach ist für die Weiterleitung eingehender Nachrichten an den Benutzerverwalter mit der Option, Kopien der Nachricht im Postfach zu belassen, konfiguriert.	Das Benutzerpostfach konnte nicht für die Weiterleitung eingehender Nachrichten an den Benutzerverwalter konfiguriert werden.
Das Benutzerpostfach konnte nicht für die Weiterleitung eingehender Nachrichten an den Benutzerverwalter konfiguriert werden. Grund: Der Benutzerverwalter ist nicht im Verzeichnis angegeben.	*Nicht zutreffend*

Berichtsabschnitt: Stammordner-Deprovisionierung

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Die Deprovisionierung des Stammordners wird übersprungen, da der Benutzer nicht über einen Stammordner verfügt.	*Nicht zutreffend*
Die Rechte des Benutzers für den Stammordner werden entfernt.	Die Rechte des Benutzers für den Stammordner konnten nicht entfernt werden.
Dem Benutzerverwalter wird Lesezugriff auf den Stammordner des Benutzers gewährt. Name des Verwalters: *Name*	Dem Benutzerverwalter konnte kein Lesezugriff auf den Stammordner des Benutzers gewährt werden. Name des Verwalters: *Name*
Nicht zutreffend	Dem Benutzerverwalter konnte kein Lesezugriff auf den Stammordner des Benutzers gewährt werden. Grund: Der Benutzerverwalter ist nicht im Verzeichnis angegeben.
In Übereinstimmung mit der Richtlinie wird beim Löschen des Benutzerkontos auch der Stammordner gelöscht. Name des Stammordners: *Name*	*Nicht zutreffend*
Den erforderlichen Benutzern und Gruppen wurde Lesezugriff auf den Stammordner des Benutzers gewährt. Liste: • *Benutzer und Gruppen*	Den erforderlichen Benutzern und Gruppen konnte kein Lesezugriff auf den Stammordner des Benutzers gewährt werden. Liste: • *Benutzer und Gruppen*
Dem Stammordner des Benutzers wird ein neuer Eigentümer zugewiesen. Name des Besitzers: *Name*	Dem Stammordner des Benutzers konnte kein neuer Besitzer zugewiesen werden. Dieser Besitzername konnte nicht festgelegt werden: *Name*

Berichtsabschnitt: Benutzerkonto-Verschiebung

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Das Benutzerkonto wird in Übereinstimmung mit der Richtlinie nicht von seinem ursprünglichen Speicherort verschoben: *Name des Containers*	*Nicht zutreffend*
Das Benutzerkonto wird an einen anderen Speicherort verschoben. Ursprünglicher Speicherort: *Name des Containers* Neuer Speicherort: *Name des Containers*	Das Benutzerkonto konnte nicht an einen anderen Speicherort verschoben werden. Ursprünglicher Speicherort: *Name des Containers* Das Verschieben an diesen Speicherort ist fehlgeschlagen: *Name des Containers*

Berichtsabschnitt: Permanentes Löschen von Benutzerkonten

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
In Übereinstimmung mit der Richtlinie wird das Löschen des Benutzerkontos nicht geplant.	*Nicht zutreffend*
Das Löschen des Benutzerkontos wird im Zeitplan festgelegt. Wird gelöscht an folgendem Datum: *Datum*	Die Löschung des Benutzerkontos konnte nicht geplant werden.
Das Benutzerkonto wurde in den Active Directory-Papierkorb verschoben.	Das Benutzerkonto konnte nicht in den Active Directory-Papierkorb verschoben werden. Überprüfen Sie, ob der Active Directory-Papierkorb aktiviert ist.

Berichtsabschnitt: Gruppenobjekt-Deprovisionierung

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Der Gruppentyp wurde von „Sicherheit" in „Verteilung" geändert.	Der Gruppentyp konnte nicht von „Sicherheit" in „Verteilung" geändert werden.
Der Gruppentyp kann nicht von „Sicherheit" in „Verteilung" geändert werden, weil die Gruppe keine Sicherheitsgruppe ist.	*Nicht zutreffend*
Die Gruppe wurde aus der globalen Adressliste (GAL) entfernt (ausgeblendet).	Die Gruppe konnte nicht aus der globalen Adressliste (GAL) entfernt (ausgeblendet) werden.
Die Gruppe kann nicht aus der globalen Adressliste (GAL) entfernt (ausgeblendet) werden, weil dies keine E-Mail-fähige Gruppe ist.	*Nicht zutreffend*
Der Gruppenname wurde geändert. Originalname: *Name* Neuer Name: *Name*	Der Gruppenname konnte nicht geändert werden. Aktueller Name: *Name* Der folgende Name konnte nicht festgelegt werden: *Name*
In Übereinstimmung mit der Richtlinie werden die Mitglieder nicht aus der Gruppe entfernt. Details: • *Liste der in der Gruppe beibehaltenen Mitglieder*	*Nicht zutreffend*
Die Mitglieder sind aus der Gruppe entfernt. Details: • *Liste der aus der Gruppe entfernten Mitglieder*	Einige Mitglieder konnten nicht aus der Gruppe entfernt werden. Details: • *Liste der aus der Gruppe entfernten Mitglieder* • *Liste der Mitglieder, die aufgrund eines Fehlers nicht aus der Gruppe entfernt wurden*
In Übereinstimmung mit der Richtlinie bleiben einige Mitglieder in der Gruppe. Details: • *Liste der aus der Gruppe entfernten Mitglieder* • *Liste der in der Gruppe beibehaltenen Mitglieder*	Einige Mitglieder konnten nicht aus der Gruppe entfernt werden. Details: • *Liste der aus der Gruppe entfernten Mitglieder* • *Liste der Mitglieder, die in Übereinstimmung mit der Richtlinie in der Gruppe beibehalten wurden* • *Liste der Mitglieder, die aufgrund eines Fehlers nicht aus der Gruppe entfernt wurden*
Die Gruppeneigenschaften wurden geändert. Liste: • *Eigenschaftsnamen, alte und neue Eigenschaftswerte*	Die Gruppeneigenschaften konnten nicht geändert werden. Liste: • *Eigenschaftsnamen, Fehlerbeschreibung*

Berichtsabschnitt: Gruppenobjekt-Verschiebung

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Die Gruppe wird in Übereinstimmung mit der Richtlinie nicht von ihrem ursprünglichen Speicherort verschoben: *Name des Containers*	*Nicht zutreffend*
Die Gruppe wird an einen anderen Speicherort verschoben. Ursprünglicher Speicherort: *Name des Containers* Neuer Speicherort: *Name des Containers*	Die Gruppe konnte nicht an einen anderen Speicherort verschoben werden. Ursprünglicher Speicherort: *Name des Containers* Das Verschieben an diesen Speicherort ist fehlgeschlagen: *Name des Containers*

Berichtsabschnitt: Dauerhaftes Löschen des Gruppenobjekts

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
In Übereinstimmung mit der Richtlinie wird das Löschen der Gruppe nicht geplant.	*Nicht zutreffend*
Das Löschen der Gruppe wird im Zeitplan festgelegt. Wird gelöscht an folgendem Datum: *Datum*	Die Löschung der Gruppe konnte nicht geplant werden.
Die Gruppe wurde in den Active Directory-Papierkorb verschoben.	Die Gruppe konnte nicht in den Active Directory-Papierkorb verschoben werden. Überprüfen Sie, ob der Active Directory-Papierkorb aktiviert ist.

Berichtsabschnitt: Benachrichtigungsverteilung

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Die Deprovisionierungsbenachrichtigung wird an die aufgeführten Empfänger gesendet (bisher nicht gesendet). Liste: • *Empfänger*	*Nicht zutreffend*
Die Deprovisionierungsbenachrichtigung wurde an die aufgeführten Empfänger gesendet. Liste: • *Empfänger*	Aufgrund eines Fehlers wurde keine Deprovisionierungs-benachrichtigung an die aufgeführten Empfänger gesendet. Liste: • *Empfänger*

Berichtsabschnitt: Berichtsverteilung

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Der Deprovisionierungsbericht wird nicht gesendet, da keine Fehler aufgetreten sind.	*Nicht zutreffend*
Der Deprovisionierungsbericht wird an die aufgeführten Empfänger gesendet (bisher nicht gesendet). Liste: • *Empfänger*	*Nicht zutreffend*
Der Deprovisionierungsbericht wurde an die aufgeführten Empfänger gesendet. Liste: • *Empfänger*	Aufgrund eines Fehlers wurde der Deprovisionierungs-bericht nicht an die aufgeführten Empfänger gesendet. Liste: • *Empfänger*

Wiederherstellen von deprovisionierten Benutzern oder Gruppen

ActiveRoles Server bietet die Möglichkeit, deprovisionierte Objekte wie etwa deprovisionierte Benutzer oder Gruppen wiederherzustellen. Der Zweck dieses Vorgangs, der als *Aufhebung der Deprovision* bezeichnet wird, besteht darin, die Änderungen rückgängig zu machen, die durch den Deprovisionsvorgang an einem Objekt vorgenommen wurden. Wenn ein deprovisioniertes Objekt wiederhergestellt werden muss (zum Beispiel wenn ein Benutzerkonto versehentlich deprovisioniert wurde), ermöglicht der Vorgang „Deprovision aufheben", das Objekt schnell wieder in den Zustand zurückzuversetzen, in dem es sich befand, bevor die Änderungen vorgenommen wurden.

Durch die Aufhebung der Deprovision werden die Änderungen rückgängig gemacht, die in Übereinstimmung mit der Standard-Deprovisionierungsrichtlinie am Objekt vorgenommen wurden. Gehen wir zum Beispiel einmal davon aus, dass eine Benutzerkonto-Deprovisionierungsrichtlinie so konfiguriert ist, dass ein deprovisioniertes Benutzerkonto folgende Merkmale aufweist:

- Das Benutzerkonto ist deaktiviert
- Das Benutzerkonto ist umbenannt
- Die Beschreibung des Benutzerkontos ist geändert
- Das Benutzerkonto verfügt über eine Reihe von deaktivierten Eigenschaften
- Das Kennwort des Benutzerkontos ist auf einen zufälligen Wert gesetzt

In diesem Fall gewährleistet die Aufhebung des Deprovisionsvorgangs,

- Dass das Benutzerkonto wieder die folgenden Merkmale aufweist:
- Die Beschreibung, der Name und andere Eigenschaften werden wieder auf die ursprünglichen Werte des Benutzerkontos zurückgesetzt
- Das Benutzerkonto bietet die Option, das Kennwort zurückzusetzen, sodass sich der Benutzer anmelden kann

Ein ähnliches Verhalten gilt für andere Richtlinien der Deprovisionierungskategorie:

- Wenn der Deprovisionsvorgang den Benutzerzugriff auf Ressourcen wie etwa den Stammordner oder das Exchange-Postfach aufhebt, dann versucht die Aufhebung des Deprovisionsvorgangs, den Benutzerzugriff auf diese Ressourcen wiederherzustellen.
- Wenn der Deprovisionsvorgang ein Benutzerkonto aus bestimmten Gruppen entfernt, dann kann die Aufhebung des Deprovisionsvorgang das Benutzerkonto zu diesen Gruppen hinzufügen und somit die Original-Gruppenmitgliedschaften des Benutzerkontos wiederherstellen.

Um ein weiteres Beispiel anzuführen, gehen wir davon aus, dass die Deprovisionierungsrichtlinie so konfiguriert ist, dass ein Deprovisionsvorgang für eine Gruppe:

- alle Mitglieder aus der Gruppe entfernt
- die Gruppe umbenennt
- die Gruppe in einen bestimmten Container verschiebt

In diesem Fall führt die Aufhebung des Deprovisionsvorgangs dazu, dass,

- die ursprüngliche Mitgliedschaftsliste der Gruppe in den Zustand zurückversetzt wird, den sie zum Zeitpunkt der Deprovisionierung aufwies,
- die Gruppe umbenannt wird, wobei der ursprüngliche Name der Gruppe wiederhergestellt wird,
- die Gruppe in den Container verschoben wird, in dem sich die Gruppe zum Zeitpunkt der Deprovisionierung befunden hat.

Ein ähnliches Verhalten gilt für andere Optionen der Richtlinie zur Deprovisionierung von Gruppen:

- Wenn der Deprovisionsvorgang die Gruppe in der Globalen Adressliste (GAL) ausblendet, stellt der Befehl „Deprovisionierung aufheben" die Sichtbarkeit der Gruppe in der GAL wieder her.
- Wenn der Deprovisionsvorgang den Gruppentyp von „Sicherheit" in „Verteilung" ändert, setzt der Befehl „Deprovisionierung aufheben" den Gruppentyp auf „Sicherheit" zurück.
- Wenn der Deprovisionsvorgang jegliche andere Eigenschaften der Gruppe ändert, stellt der Befehl „Deprovisionierung aufheben" die ursprünglichen Eigenschaftswerte wieder her.

Sowohl die ActiveRoles Server-Konsole als auch das Web-Interface stellen den Befehl **Deprovisionierung aufheben** für deprovisionierte Benutzer oder Gruppen bereit. Wenn dieser Befehl für ein deprovisioniertes Objekt ausgewählt wird, sendet er eine Anforderung zur Wiederherstellung des Objekts. Bei Erhalt der Anforderung führt ActiveRoles Server alle erforderlichen Vorgänge durch, um die Ergebnisse der Deprovisionierung des Objekts rückgängig zu machen, und erstellt einen detaillierten Bericht über die durchgeführten Vorgänge. Dieser Bericht enthält außerdem Informationen über den Erfolg oder Misserfolg jedes Vorgangs.

Richtlinienoptionen für die Aufhebung der Deprovisionierung eines Benutzers

Das Verhalten der Aufhebung des Deprovisionsvorgangs wird durch eine konfigurierbare Richtlinie bestimmt, die in einem integrierten Richtlinienobjekt enthalten ist. Hierbei handelt es sich um das Richtlinienobjekt mit dem Namen **Built-in Policy – Default Rules to Undo User Deprovisioning**. Sie befindet sich im Container **Builtin** unter **Configuration/Policies/Administration**. Das Richtlinienobjekt wird auf den Ordner **Active Directory** angewendet und wirkt sich daher auf alle Domänen aus, die bei ActiveRoles Server registriert sind (verwaltete Domänen).

Die von dieser Richtlinie bereitgestellte Option kann verwendet werden, um die Wiederherstellung von Gruppenmitgliedschaften und das Rücksetzen des Benutzerkennworts zu verhindern:

- **Gruppenmitgliedschaften wiederherstellen** Bei Auswahl dieser Option führt die Aufhebung des Deprovisionsvorgangs für ein deprovisioniertes Benutzerkonto zum Hinzufügen des Kontos zu den Verteiler- und Sicherheitsgruppen, aus denen das Konto in Übereinstimmung mit der Richtlinie zum Entfernen von Gruppenmitgliedschaften entfernt wurde. Wenn Sie nicht möchten, dass wiederhergestellte Konten automatisch zu Gruppen hinzugefügt werden, dann deaktivieren Sie diese Option.

  Beachten Sie, dass unabhängig davon, ob diese Option aktiviert oder deaktiviert ist, ActiveRoles Server, sobald ein deprovisioniertes Benutzerkonto wiederhergestellt wird, das Konto abhängig von seinen Eigenschaften automatisch zu den entsprechenden dynamischen Gruppen und Gruppenfamilien hinzufügt.

- **Kennwort unverändert lassen** Führt dazu, dass die Aufhebung des Deprovisionsvorgangs für ein deprovisioniertes Benutzerkonto das Rücksetzen des Kennworts für das wiederhergestellte Konto verhindert. Aktivieren Sie diese Option, wenn Sie möchten, dass das Kennwort vom Help Desk oder mit Hilfe einer Selfservice-Kennwortverwaltungslösung wiederhergestellt wird, nachdem das Konto wiederhergestellt wurde.
- **Zum Rücksetzen des Kennworts auffordern** Führt dazu, dass die Aufhebung des Deprovisionsvorgangs für ein deprovisioniertes Benutzerkonto das Rücksetzen des Kennworts für das wiederhergestellte Konto ermöglicht. Wenn diese Option ausgewählt ist, zeigt der Befehl **Deprovisionierung aufheben** ein Dialogfeld an, in dem das Kennwort zurückgesetzt werden kann.

Gehen Sie folgendermaßen vor, um die Richtlinienoptionen anzuzeigen oder zu ändern:

1. Öffnen Sie die ActiveRoles Server-Konsole.
2. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration | Policies | Administration** und wählen Sie dann **Builtin** unter **Administration**.
3. Doppelklicken Sie im Bereich „Details" auf **Built-in Policy – Default Rules to Undo User Deprovisioning**.
4. Klicken Sie auf der Registerkarte **Richtlinien** im Dialogfeld **Eigenschaften** auf die Richtlinie in der Liste und klicken Sie dann auf **Anzeigen/Bearbeiten**, um auf die Richtlinienoptionen zuzugreifen.

Da das integrierte Richtlinienobjekt normalerweise auf den Active Directory-Knoten im ActiveRoles Server-Namespace angewandt wird, gelten die Richtlinienoptionen für alle deprovisionierten Benutzerkonten. Wenn Sie verschiedene Richtlinienoptionen für unterschiedliche Domänen oder Container benötigen, erstellen Sie eine Kopie des integrierten Richtlinienobjekts, konfigurieren Sie dann die Kopie entsprechend und wenden Sie sie dann wie gewünscht an.

Die Aufhebung des Deprovisionsvorgangs ist normalerweise in allen bei ActiveRoles Server registrierten Domänen aktiviert. Es ist möglich, diesen Vorgang in einzelnen Domänen oder Containern oder in allen Domänen zu verhindern, indem Sie die Richtlinie sperren oder deaktivieren, die den Vorgang regelt. Bei Deaktivierung des integrierten Richtlinienobjekts kann eine aktivierte Kopie dieses Richtlinienobjekts angewandt werden, um die Aufhebung des Deprovisionsvorgangs in einzelnen Domänen oder Containern zu ermöglichen.

Delegieren der Aufhebung der Deprovision

Das Recht zur Wiederherstellung von deprovisionierten Benutzern oder Gruppen besitzt standardmäßig das Administratorkonto „AR Server Admin", das während der Installation von ActiveRoles Server angegeben wird. Diese Aufgabe kann jedoch an jede beliebigen Gruppe oder jeden beliebigen Benutzer delegiert werden. Es wird eine ausschließlich für diesen Zweck vorgesehene Zugriffsvorlage bereitgestellt, damit Sie die Verwendung des Befehls **Deprovisionierung aufheben** delegieren können, ohne zugleich die Rechte für den Erstellungs- oder Löschvorgang zu delegieren.

Um die Wiederherstellung deprovisionierter Benutzer oder Gruppen, die sich in einem bestimmten Container wie etwa in einer Organisationseinheit oder einer verwalteten Einheit befinden, zu delegieren, wenden Sie die Zugriffsvorlage wie folgt an:

Gehen Sie folgendermaßen vor, um die Aufhebung der Deprovision zu delegieren:

1. Klicken Sie in der ActiveRoles Server-Konsole mit der rechten Maustaste auf den Container und klicken Sie dann auf **Kontrolle delegieren**, um das Fenster **ActiveRoles Server-Sicherheit** anzuzeigen.
2. Klicken Sie im Fenster **ActiveRoles Server-Sicherheit** auf **Hinzufügen**, um den Assistenten „Delegation der Kontrolle" zu starten. Klicken Sie auf **Weiter**.
3. Klicken Sie auf der Seite **Benutzer oder Gruppen** auf **Hinzufügen**, und wählen Sie dann die Benutzer oder Gruppen aus, an die Sie die Rechte für die Aufgabe delegieren möchten. Klicken Sie auf **Weiter**.
4. Erweitern Sie auf der Seite **Zugriffsvorlagen** den Ordner **Active Directory** und gehen Sie dann wie folgt vor:
   - Um die Aufgabe der Wiederherstellung von deprovisionierten Benutzern zu delegieren, aktivieren Sie das Kontrollkästchen neben **Benutzer – Aufgabe der Aufhebung der Deprovision durchführen**.
   - Um die Aufgabe der Wiederherstellung von deprovisionierten Gruppen zu delegieren, aktivieren Sie das Kontrollkästchen neben **Gruppen – Aufgabe der Aufhebung der Deprovision durchführen**.
5. Klicken Sie auf **Weiter** und befolgen Sie die Anweisungen im Assistenten; übernehmen Sie bei diesem Vorgang die Standardeinstellungen.

Nachdem Sie diese Schritte abgeschlossen haben, sind die in Schritt 3 ausgewählten Benutzer und Gruppen autorisiert, die Deprovision von Benutzern in dem in Schritt 1 ausgewählten Container und ggf. in allen seinen Untercontainern zurückzunehmen.

Verwenden des Befehls zur Aufhebung der Deprovision

Der Befehl **Deprovisionierung aufheben** steht über die Konsole und das Web-Interface von ActiveRoles Server den Benutzern zur Verfügung, die zum Wiederherstellen von deprovisionierten Benutzern oder Gruppen autorisiert sind. Bei Verwendung dieses Befehls starten Sie die Aufhebung des Deprovisionsvorgangs für die von Ihnen ausgewählten Objekte, wodurch ActiveRoles Server die Ergebnisse der Deprovisionierung dieser Objekte rückgängig macht.

Gehen Sie folgendermaßen vor, um ein deprovisioniertes Benutzerkonto wiederherzustellen:

1. Klicken Sie in der ActiveRoles Server-Konsole mit der rechten Maustaste auf das Benutzerkonto und klicken Sie dann auf **Deprovisionierung aufheben**.
2. Wählen Sie im Dialogfeld **Kennwortoptionen** die Optionen, die auf das Kennwort des wiederhergestellten Kontos angewandt werden sollen, und klicken Sie dann auf **OK**.

   *Für weitere Informationen zu jeder Option öffnen Sie das Dialogfeld **Kennwortoptionen** und drücken Sie dann auf F1.*
3. Warten Sie, während ActiveRoles Server das Benutzerkonto wiederherstellt.

Gehen Sie folgendermaßen vor, um eine deprovisionierte Gruppe wiederherzustellen:

1. Klicken Sie in der ActiveRoles Server-Konsole mit der rechten Maustaste auf die Gruppe und klicken Sie dann auf **Deprovisionierung aufheben**.
2. Warten Sie, während ActiveRoles Server die Gruppe wiederherstellt.

Der Fortschritt des Vorgangs und die Ergebnisse werden im Fenster **Ergebnisse der Aufhebung der Deprovisionierung** angezeigt, das dem weiter oben in diesem Kapitel beschriebenen Fenster **Deprovisionsergebnisse** entspricht. Nach Abschluss des Vorgangs wird in dem Fenster die Vorgangszusammenfassung angezeigt, sodass Sie die Vorgangsergebnisse detailliert untersuchen können.

Bericht über die Ergebnisse der Aufhebung der Deprovisionierung

Für jedes wiederhergestellte Objekt können Sie im Fenster **Ergebnisse der Aufhebung der Deprovisionierung** die Ergebnisse des Wiederherstellungsvorgangs für dieses Objekt untersuchen. Die ActiveRoles Server-Konsole oder das Web-Interface öffnet das Fenster **Ergebnisse der Aufhebung der Deprovisionierung**, wenn sie bzw. es den Befehl **Deprovisionierung aufheben** ausführt.

Im Fenster **Ergebnisse der Aufhebung der Depovisionierung** wird ein Bericht über die Aufhebung des Deprovisionsvorgangs angezeigt, das dem weiter oben in diesem Kapitel beschriebenen, im Zusammenhang mit der Deprovisionierung stehenden Bericht entspricht. In dem Bericht sind Vorgangsergebnisse in Abschnitte gegliedert, wobei jeder Abschnitt Berichtselemente, die zu einer bestimmten Deprovisionierungsrichtlinienkategorie gehören, enthält. Die Berichtselemente innerhalb eines bestimmten Abschnitts geben Auskunft über die Vorgänge, die durchgeführt wurden, um die Änderungen rückgängig zu machen, die von der Deprovisionierungsrichtlinie der entsprechenden Kategorie vorgenommen wurden.

Wenn Sie oben im Bericht auf die Überschrift klicken, wird der Bericht vollständig erweitert, und alle Berichtselemente werden angezeigt. Sie können auch einzelne Abschnitte in dem Bericht erweitern oder ausblenden, indem Sie auf die Überschrift des jeweiligen Berichts klicken.

Für bestimmte Elemente steht im Bericht die Option zur Verfügung, die Ansicht weiter zu erweitern und zusätzliche Informationen anzuzeigen. Durch Anklicken der Option **Liste** wird eine Liste von Elementen (z.B. Benutzer- oder Gruppeneigenschaften) anzeigen, die an dem Vorgang beteiligt sind. Indem Sie auf die Option **Details** klicken, können Sie das Vorgangsergebnis detaillierter untersuchen.

Das Fenster **Ergebnisse der Aufhebung der Deprovisionierung** bietet auch die Möglichkeit, alle Vorgangsergebnisse in einer Datei für den Druck oder die Anzeige zu dokumentieren. Mit dem Kontextmenü können Sie den Bericht in eine Datei im HTML- oder XML-Format exportieren, ihn drucken oder über E-Mail versenden.

Berichtsinhalt

In den folgenden Tabellen sind die möglichen Berichtselemente aufgelistet. Es ist eine Tabelle pro Berichtsabschnitt vorhanden. Die Elemente in den einzelnen Abschnitten beschreiben die Ergebnisse der Aktionen, die ausgeführt wurden, um die von der entsprechenden Deprovisionierungsrichtlinie vorgenommenen Änderungen rückgängig zu machen. Berichtselemente enthalten außerdem Informationen zum Erfolg oder Fehler jeder Aktion. Bei einem Fehler enthält das Berichtselement eine Fehlerbeschreibung.

Nicht alle aufgelisteten Elemente müssen notwendigerweise in einem Bericht enthalten sein. Ein Bericht umfasst nur Berichtselemente, die in Zusammenhang mit den Deprovisionierungsrichtlinien stehen, die gültig waren, als der Benutzer oder die Gruppe deprovisioniert wurde.

Berichtsabschnitt: Benutzerkontodeprovisionierung aufheben

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Das Benutzerkonto ist aktiviert.	Das Benutzerkonto konnte nicht aktiviert werden.
Das Benutzerkennwort wird auf einen bekannten Wert mit den folgenden Kennwortoptionen zurückgesetzt: *<Liste der Optionen>*	Zurücksetzen des Benutzerkennworts fehlgeschlagen.
Das aktuelle Benutzerkennwort bleibt unverändert.	*Nicht zutreffend*
Der Benutzername wird wiederhergestellt. Alter Name: *Name* Wiederhergestellter Name: *Name*	Der Benutzername konnte nicht wiederhergestellt werden. Aktueller Name: *Name* Der folgende Name konnte nicht festgelegt werden: *Name*
Die Benutzereigenschaften werden wiederhergestellt. Liste: • *Benutzereigenschaften, neue Eigenschaftswerte*	Die Benutzereigenschaften konnten nicht wiederhergestellt werden. Liste: • *Benutzereigenschaften, Fehlerbeschreibung*

Berichtsabschnitt: Entfernen der Gruppenmitgliedschaft rückgängig machen

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
In Übereinstimmung mit der Richtlinie wird die Mitgliedschaft des Benutzers in Sicherheitsgruppen nicht wiederhergestellt.	*Nicht zutreffend*
In Übereinstimmung mit der Richtlinie wird die Mitgliedschaft des Benutzers in Verteilergruppen oder E-Mail-fähigen Sicherheitsgruppen nicht wiederhergestellt.	*Nicht zutreffend*
Die Mitgliedschaft des Benutzers in Sicherheitsgruppen wird wiederhergestellt. Details: • *Sicherheitsgruppen, zu denen der Benutzer hinzugefügt wird*	Die Mitgliedschaft des Benutzers in einigen Sicherheitsgruppen konnte nicht wiederhergestellt werden. Details: • *Sicherheitsgruppen, zu denen der Benutzer hinzugefügt wird* • *Sicherheitsgruppen, zu denen der Benutzer aufgrund eines Fehlers nicht hinzugefügt wird*
Die Mitgliedschaft des Benutzers in Verteilergruppen und E-Mail-fähigen Sicherheitsgruppen wird wiederhergestellt. Details: • *Verteilergruppen und E-Mail-fähige Sicherheitsgruppen, zu denen der Benutzer hinzugefügt wird*	Die Mitgliedschaft des Benutzers in einigen Verteilergruppen oder E-Mail-fähigen Sicherheitsgruppen konnte nicht wiederhergestellt werden. Details: • *Verteilergruppen und E-Mail-fähige Sicherheitsgruppen, zu denen der Benutzer hinzugefügt wird* • *Verteilergruppen oder E-Mail-fähige Sicherheitsgruppen, zu denen der Benutzer aufgrund eines Fehlers nicht hinzugefügt wird*

Berichtsabschnitt: Exchange-Postfach-Deprovisionierung aufheben

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Die Wiederherstellung des Benutzerpostfachs wird übersprungen, da der Benutzer zum Zeitpunkt der Deprovisionierung über kein Exchange-Postfach verfügte.	*Nicht zutreffend*
Der ursprüngliche Zustand des Benutzerpostfachs wird in der Globalen Adressliste (GAL) wiederhergestellt.	Der ursprüngliche Zustand des Benutzerpostfachs in der Globalen Adressliste (GAL) konnte nicht wiederhergestellt werden.
Die ursprünglichen Einstellungen für das Senden von Nichtzustellbarkeitsberichten werden für das Benutzerpostfach wiederhergestellt.	Die ursprünglichen Einstellungen für das Senden von Nichtzustellbarkeitsberichten konnten nicht für das Benutzerpostfach wiederhergestellt werden.
Die ursprüngliche Konfiguration der E-Mail-Weiterleitung für das Benutzerpostfach wird wiederhergestellt.	Die ursprüngliche Konfiguration der E-Mail-Weiterleitung für das Benutzerpostfach konnte nicht wiederhergestellt werden.
Die ursprünglichen Sicherheitseinstellungen werden im Benutzerpostfach wiederhergestellt.	Die ursprünglichen Sicherheitseinstellungen im Benutzerpostfach konnten nicht wiederhergestellt werden.

Berichtsabschnitt: Stammordner-Deprovisionierung aufheben

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Die Wiederherstellung des Stammordners wird übersprungen, da der Benutzer zum Zeitpunkt der Deprovisionierung über keinen Stammordner verfügte.	*Nicht zutreffend*
Die ursprünglichen Sicherheitseinstellungen werden im Stammordner des Benutzers wiederhergestellt.	Die ursprünglichen Sicherheitseinstellungen im Stammordner des Benutzers konnten nicht wiederhergestellt werden.

Berichtsabschnitt: Benutzerkonto-Verschiebung rückgängig machen

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Es wurden keine rückgängig zu machenden Änderungen vorgenommen.	*Nicht zutreffend*
Das Benutzerkonto wird an seinen ursprünglichen Speicherort verschoben. Ehemaliger Speicherort: *Name des Containers* Wiederhergestellter ursprünglicher Speicherort: *Name des Containers*	Das Benutzerkonto konnte nicht an seinen ursprünglichen Speicherort verschoben werden. Aktueller Speicherort: *Name des Containers* Das Verschieben an diesen Speicherort ist fehlgeschlagen: *Name des Containers*

Berichtsabschnitt: Permanentes Löschen des Benutzerkontos rückgängig machen

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Es wurden keine rückgängig zu machenden Änderungen vorgenommen.	*Nicht zutreffend*
Die geplante Löschung des Benutzerkontos wird abgebrochen.	Der Abbruch der geplanten Löschung des Benutzerkontos ist fehlgeschlagen. Das Konto wird an diesem Datum gelöscht: *Datum*

Berichtsabschnitt: Deprovisionierung des Gruppenobjekts rückgängig machen

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Der Gruppentyp wurde wieder in „Sicherheitsgruppe" zurück geändert.	Der Gruppentyp konnte nicht wieder in „Sicherheit" geändert werden.
Die Gruppe wurde in der globalen Adressliste (GAL) wiederhergestellt.	Die Gruppe konnte nicht in der globalen Adressliste (GAL) wiederhergestellt werden.
Der Gruppenname wird wiederhergestellt. Alter Name: *Name* Wiederhergestellter Name: *Name*	Der Gruppenname konnte nicht wiederhergestellt werden. Aktueller Name: *Name* Der folgende Name konnte nicht festgelegt werden: *Name*
Die Mitgliedschaftsliste der Gruppe ist wiederhergestellt. Details: • *Liste der zur Gruppe hinzugefügten Mitglieder*	Die Mitgliederliste der Gruppe konnte nicht wiederhergestellt werden. Details: • *Liste der zur Gruppe hinzugefügten Mitglieder* • *Liste der Mitglieder, die aufgrund eines Fehlers nicht zur Gruppe hinzugefügt wurden*
Die Gruppeneigenschaften wurden wiederhergestellt. Liste: • *Gruppeneigenschaften, neue Eigenschaftswerte*	Die Gruppeneigenschaften konnten nicht wiederhergestellt werden. Liste: • *Gruppeneigenschaften, Fehlerbeschreibung*

Berichtsabschnitt: Verschieben des Gruppenobjekts rückgängig machen

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Es wurden keine rückgängig zu machenden Änderungen vorgenommen.	*Nicht zutreffend*
Die Gruppe wird an ihren ursprünglichen Speicherort verschoben. Ehemaliger Speicherort: *Name des Containers* Wiederhergestellter ursprünglicher Speicherort: *Name des Containers*	Die Gruppe konnte nicht an ihren ursprünglichen Speicherort verschoben werden. Aktueller Speicherort: *Name des Containers* Das Verschieben an diesen Speicherort ist fehlgeschlagen: *Name des Containers*

Berichtsabschnitt: Dauerhaftes Löschen des Gruppenobjekts rückgängig machen

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Es wurden keine rückgängig zu machenden Änderungen vorgenommen.	*Nicht zutreffend*
Die geplante Löschung der Gruppe wurde abgebrochen.	Der Abbruch der geplanten Löschung der Gruppe ist fehlgeschlagen. Die Gruppe wird an diesem Datum gelöscht: *Datum*

Richtlinie zur Vermeidung einer Containerlöschung

Wenn ein Administrator ein Containerobjekt wie etwa eine Organisationseinheit, die über untergeordnete Objekte verfügt, auswählt und löscht, kann es zu einem Massenlöschvorgang kommen. Obwohl Massenlöschungen selten sind, sind dies Ereignisse, die zu einer Unterbrechung des Betriebs führen und gegen die Sie sich schützen können, indem Sie eine neue Richtlinie nutzen: der Containerlöschschutz.

Einer der am häufigsten vorkommenden Massenlöschvorgänge ist das Löschen eines Containers. Dieses Ereignis kann eintreten, wenn ActiveRoles Server verwendet wird, um ein Containerobjekt zu löschen, das andere (untergeordnete) Objekte enthält. Standardmäßig weist eine Containerlöschung die folgenden Merkmale auf:

- Zunächst erstellt ActiveRoles Server eine Liste aller im Container gefundenen Objekte (untergeordnete Objekte) und startet dann nacheinander die Löschung der aufgeführten Objekte.
- Dann führt ActiveRoles Server für jedes Objekt in der Liste eine Zugriffskontrolle durch, um zu ermitteln, ob der Benutzer oder Prozess, der die Löschung angefordert hat, über ausreichende Rechte zum Löschen des Objekts verfügt. Wenn die Zugriffskontrolle den Löschvorgang zulässt, dann wird das Objekt gelöscht. Andernfalls löscht ActiveRoles Server das Objekt nicht und setzt den Löschvorgang mit dem nächsten Objekt in der Liste fort.
- Wenn alle untergeordneten Objekte gelöscht sind, löscht ActiveRoles Server den Container selbst. Wenn irgendwelche der untergeordneten Objekte nicht gelöscht wurden (zum Beispiel aufgrund von unzureichenden Rechte zum Löschen seitens der anfordernden Instanz), wird der Container ebenfalls nicht gelöscht.

Als Folge dieses Verhaltens kann ein Administrator, der über einen Vollzugriff auf eine Organisationseinheit in ActiveRoles Server verfügt, versehentlich die gesamte Organisationseinheit mit all ihren Inhalten in einem einzigen Vorgang löschen. Um dies zu verhindern, bietet ActiveRoles Server eine bestimmte Richtlinie, die das Löschen von nicht leeren Containern verhindert.

Die Richtlinie zur Vermeidung einer Containerlöschung definiert eine konfigurierbare Liste der Namen von Objekttypen wie durch das Active Directory-Schema angegeben (zum Beispiel der Objekttyp „Organisationseinheit"). Wenn ein ActiveRoles Server-Client die Löschung eines bestimmten Containers anfordert, wertet der Verwaltungsdienst die Anforderung aus, um zu ermitteln, ob sich der Containertyp in der von dieser Richtlinie definierten Liste befindet. Wenn sich der Containertyp in der Liste befindet und der Container irgendwelche Objekte enthält, verweigert der Verwaltungsdienst die Anforderung und verhindert somit die Löschung des Containers. In diesem Fall fordert der Client den Benutzer auf, alle in dem Container befindlichen Objekte zu löschen, bevor versucht wird, den Container selbst zu löschen.

Gehen Sie folgendermaßen vor, um eine Richtlinie zur Vermeidung einer Containerlöschung zu konfigurieren:

1. Wählen Sie in der Konsolenstruktur **Configuration | Policies | Administration | Builtin**.
2. Doppelklicken Sie im Bereich „Details" auf **Built-in Policy – Container Deletion Prevention**.
3. Wählen Sie auf der Registerkarte **Richtlinien** die Richtlinie aus der Liste aus und klicken Sie dann auf **Anzeigen/Bearbeiten**.

4. Gehen Sie auf der Registerkarte **Containertypen** wie folgt vor:
   a) Klicken Sie auf **Hinzufügen**.
   b) Wählen Sie im Dialogfeld **Objekttyp auswählen** die Containertypen aus, die Sie schützen möchten, und klicken Sie dann auf **OK**.

   So können Sie zum Beispiel den Objekttyp „Organisationseinheit" auswählen, um das Löschen von nicht leeren Organisationseinheiten zu verhindern.
5. Klicken Sie auf **OK**, um die von Ihnen geöffneten Dialogfelder zu schließen.

Das integrierte Richtlinienobjekt, das Sie mit Hilfe der oben aufgeführten Anweisungen konfiguriert haben, verhindert die Löschung von nicht leeren Containern in jeder beliebigen verwalteten Domäne.

Es kann erforderlich sein, dass ActiveRoles Server das Löschen von nicht leeren Containern, die sich außerhalb eines bestimmten Bereichs befinden (wie etwa eine bestimmte Domäne, Organisationseinheit oder verwaltete Einheit) nicht verhindern soll, während das Löschen von nicht leeren Containern, die in diesen bestimmten Bereich fallen, verhindert werden soll. In diesem Szenario müssen Sie eine Kopie des integrierten Richtlinienobjekts erstellen und konfigurieren und diese Kopie dann auf den betreffenden Bereich anwenden. Blockieren Sie dann die Auswirkungen des integrierten Richtlinienobjekts, indem Sie das Kontrollkästchen **Alle in diesem Kontrollkästchenobjekt enthaltenen Richtlinien deaktivieren** auf der Registerkarte **Richtlinien** im Dialogfeld für die Verwaltung der Eigenschaften des Richtlinienobjekts aktivieren.

Wenn Sie nur das Löschen von nicht leeren Containern innerhalb eines bestimmten Bereichs zulassen möchten, dann können Sie einfach die Auswirkungen des integrierten Richtlinienobjekts auf das Objekt, das für den betreffenden Bereich steht, blockieren. Wenn Sie also das Löschen von Organisationseinheiten zulassen möchten, die in eine bestimmte verwaltete Einheit fallen, können Sie den Befehl **Richtlinie erzwingen** auf diese verwaltete Einheit anwenden, um das Dialogfeld für die Verwaltung von Richtlinieneinstellungen anzuzeigen und um dann das Kontrollkästchen **Gesperrt** neben dem Namen des integrierten Richtlinienobjekts zu aktivieren.

Erweiterungsfähigkeit von Richtlinien

In ActiveRoles Server können Administratoren mit ActiveRoles Server installierte vordefinierte Richtlinien konfigurieren. Standardmäßig enthält die Liste der Richtlinientypen in der ActiveRoles Server-Konsole nur die vordefinierten Typen wie etwa **Automatische Stammordner-Bereitstellung** oder **Benutzerkontodeprovisionierung**. Es ist möglich, die Liste durch Hinzufügen neuer Richtlinientypen zu erweitern.

Jeder Richtlinientyp legt einen bestimmten Richtlinienvorgang (zum Beispiel die Erstellen eines Stammordners für ein Benutzerkonto) zusammen mit einer Reihe von Richtlinienparametern fest, um den Richtlinienvorgang zu konfigurieren (zum Beispiel Parameter, die den Netzwerkspeicherort angeben, an dem die Stammordner erstellt werden sollen). ActiveRoles Server ermöglicht die Implementierung und Bereitstellung von benutzerdefinierten Richtlinientypen. ActiveRoles Server ermöglicht die Erstellung von benutzerdefinierten Richtlinientypen sowie die Auflistung zusammen mit den vordefinierten Richtlinientypen, was den Administratoren ermöglicht, Richtlinien zu konfigurieren, die von diesen neuen Richtlinientypen festgelegte benutzerdefinierte Vorgänge durchführen.

ActiveRoles Server ermöglicht die Erstellung von benutzerdefinierten Richtlinien, die auf dem integrierten Richtlinientyp „Skriptausführung" basieren. Die Erstellung und Konfiguration einer Skriptrichtlinie von Grund auf kann jedoch zeitaufwändig sein. Benutzerdefinierte Richtlinientypen bieten eine Möglichkeit, dieses zeitaufwändige Verfahren abzukürzen. Sobald ein benutzerdefinierter Richtlinientyp bereitgestellt ist, der auf ein bestimmtes Skript verweist, können Administratoren auf einfache Weise Richtlinien dieses Typs konfigurieren und anwenden, sodass diese Richtlinien die von diesem Skript vorgegebenen Vorgänge ausführen. Das Richtlinienskript definiert auch die für den Richtlinientyp spezifischen Richtlinienparameter.

Benutzerdefinierte Richtlinientypen bieten einen erweiterbaren Mechanismus für die Bereitstellung von benutzerdefinierten Richtlinien. Diese Möglichkeit wird über die Objektklasse „Richtlinientyp" implementiert. Richtlinientyp-Objekte können mit Hilfe der ActiveRoles Server-Konsole erstellt werden, wobei jedes Objekt einen bestimmten benutzerdefinierten Richtlinientyp angibt.

Designelemente

Die Richtlinien-Erweiterungsfunktion stützt sich auf zwei Interaktionen: Richtlinientyp-Bereitstellung und Richtlinientyp-Nutzung.

Richtlinientyp-Bereitstellung

Das Bereitstellungsverfahren umfasst die Entwicklung eines Skripts, das die Richtlinienaktion implementiert und die Richtlinienparameter deklariert; die Erstellung eines Skriptmoduls, das das Skript enthält; und die Erstellung eines Richtlinientypobjekts, das sich auf dieses Skriptmodul bezieht. Um einen Richtlinientyp in einer anderen Umgebung bereitzustellen, kann ein Administrator den Richtlinientyp in eine Exportdatei in der Quellumgebung exportieren und die Datei dann in die Zielumgebung importieren. Die Verwendung von Exportdateien erleichert die Verbreitung von benutzerdefinierten Richtlinientypen.

Richtlinientyp-Nutzung

Die Richtlinientyp-Nutzung ist der Prozess der Konfiguration von Richtlinien. Dieser Prozess läuft ab, wenn ein Administrator ein neues Richtlinienobjekt erstellt oder Richtlinien zu einem vorhandenen Richtlinienobjekt hinzufügt. Der Assistent für die Erstellung eines Richtlinienobjekt umfasst zum Beispiel eine Seite, die zur Auswahl einer Richtlinie auffordert. Auf der Seite werden die in ActiveRoles Server definierten Richtlinientypen einschließlich der benutzerdefinierten Richtlinientypen aufgelistet. Wenn ein benutzerdefinierter Richtlinientyp ausgewählt wird, bietet der Assistent eine Seite für die Konfiguration der für diesen Richtlinientyp spezifischen Richtlinienparameter an. Nach Fertigstellung des Assistenten enthält das Richtlinienobjekt eine voll funktionsfähige Richtlinie des ausgewählten benutzerdefinierten Typs.

ActiveRoles Server bietet eine grafische Benutzeroberfläche einschließlich einer programmierbaren Schnittstelle für die Erstellung und Verwaltung von benutzerdefinierten Richtlinientypen. Mit Hilfe dieser Schnittstellen können ActiveRoles Server-Richtlinien erweitert werden, um den Anforderungen einer bestimmten Umgebung zu entsprechen. ActiveRoles Server verfügt weiterhin über einen Bereitstellungsmechanismus, mit dem Administratoren neue Richtlinientypen in Betrieb nehmen können.

Da die Richtlinienerweiterung zwei Interaktionen umfasst, bietet ActiveRoles Server Lösungen auf beiden Gebieten. Der Verwaltungsdienst behält die Richtlinientypdefinitionen bei und stellt die Richtlinientypen seinen Clients wie etwa der ActiveRoles Server-Konsole oder ADSI Provider bereit. Die Konsole kann für folgende Vorgänge verwendet werden:

- Erstellen eines neuen benutzerdefinierten Richtlinientyps, entweder von Grund auf oder per Import eines Richtlinientyps, der aus einer anderen Umgebung exportiert wurde.
- Vornehmen von Änderungen an der Definition eines vorhandenen benutzerdefinierten Richtlinientyps.
- Hinzufügen einer Richtlinie eines bestimmten benutzerdefinierten Typs zu einem Richtlinienobjekt, wodurch die erforderlichen Änderungen an den von der Richtlinientypdefinition bereitgestellten Richtlinienparametern vorgenommen werden.

Normalerweise entwickelt ein ActiveRoles Server-Experte einen benutzerdefinierten Richtlinientyp in einer separaten Umgebung und exportiert dann den Richtlinientyp in eine Exportdatei. Ein ActiveRoles Server-Administrator stellt dann den Richtlinientyp durch Import der Exportdatei in der Produktionsumgebung bereit. Anschließend kann die ActiveRoles Server-Konsole für die Konfiguration und Anwendung der Richtlinien dieses neuen Typs verwendet werden.

Richtlinientypobjekte

Die Richtlinienerweiterbarkeit beruht auf Richtlinientypobjekten, von denen jedes einen einzigen Richtlinientyp angibt. Richtlinientypobjekte werden sowohl bei der Richtlinientyp-Bereitstellung als auch bei der Richtlinientyp-Nutzung verwendet. Der Prozess der Bereitstellung eines neuen Richtlinientyps umfass die Erstellung eines Richtlinientypobjekts. Während des Hinzufügens einer benutzerdefinierten Richtlinie wird die Richtlinientypdefinition vom entsprechenden Richtlinientypobjekt abgerufen.

Jedes Richtlinientypobjekt enthält die folgenden Daten für die Definition eines einzelnen Richtlinientyps:

- **Anzeigename** Gibt den von diesem Richtlinientypobjekt dargestellten Richtlinientyp an. Dieser Name wird auf der Assistentenseite angezeigt, auf der Sie eine zu konfigurierende Richtlinie auswählen, wenn Sie ein neues Richtlinienobjekt erstellen oder eine Richtlinie zu einem vorhandenen Richtlinienobjekt hinzufügen.

- **Beschreibung** Ein Text, der den Richtlinientyp beschreibt. Dieser Text wird angezeigt, wenn Sie den Richtlinientyp im Assistenten zur Erstellung eines neuen Richtlinienobjekts oder im Assistenten zum Hinzufügen einer Richtlinie zu einem vorhandenen Richtlinienobjekt auswählen.
- **Verweis auf ein Skriptmodul** Gibt das Skript an, das bei der Ausführung einer Richtlinie dieses Typs ausgeführt werden soll. Wenn Sie eine Richtlinie eines benutzerdefinierten Richtlinientyps hinzufügen, erstellen Sie effektiv eine Richtlinie, die das Skript aus dem Skriptmodul ausführt, das vom entsprechenden Richtlinientypobjekt angegeben wird.
- **Richtlinientypkategorie** Gibt die Kategorie des Richtlinienobjekts an, zu dem eine Richtlinie dieses Typs hinzugefügt werden kann. Für einen Richtlinientyp kann die Kategorieoption entweder auf „Bereitstellung" oder „Deprovisionierung" gesetzt sein, was das Hinzufügen von Richtlinien dieses Typs zu Bereitstellungs- bzw. Deprovisionsrichtlinienobjekten ermöglicht.
- **Richtlinientypsymbol** Das Bild, das neben dem Anzeigenamen des Richtlinientyps auf der Assistentenseite angezeigt wird, auf der Sie eine zu konfigurierende Richtlinie auswählen, um die Identifizierung und visuelle Unterscheidung dieses Richtlinientyps von anderen Richtlinientypen zu erleichtern.

Um einen benutzerdefinierten Richtlinientyp zu erstellen, müssen Sie zunächst ein Skriptmodul erstellen, das das Richtlinienskript enthält. Dann können Sie ein Richtlinientypobjekt erstellen, das auf dieses Skriptmodul verweist. Wenn Sie einen Richtlinientyp importieren, erstellt ActiveRoles Server automatisch sowohl das Skriptmodul als auch das Richtlinientypobjekt für diesen Richtlinientyp. Nach der Erstellung des Richtlinientypobjekts können Sie eine Richtlinie dieses neuen Typs zu einem Richtlinienobjekt hinzufügen.

Erstellen und Verwalten von benutzerdefinierten Richtlinientypen

In ActiveRoles Server bieten Richtlinientypobjekte die Möglichkeit, die Definition eines benutzer-definierten Richtlinientyps in einem einzelnen Objekt zu speichern. Richtlinientypobjekte können exportiert und importiert werden. Dies erleichtert die Verbreitung von benutzerdefinierten Richtlinien in anderen Umgebungen.

Wenn Sie ein neues Richtlinienobjekt erstellen oder eine Richtlinie zu einem vorhandenen Richtlinienobjekt hinzufügen, wird einem Administrator eine Liste der von den Richtlinientypobjekten abgeleiteten Richtlinientypen angezeigt. Bei Auswahl eines benutzerdefinierten Richtlinientyps aus der Liste erstellt ActiveRoles Server eine Richtlinie auf der Grundlage der im entsprechenden Richtlinientypobjekt gefundenen Einstellungen.

Dieser Abschnitt deckt die folgenden, für benutzerdefiniert Richtlinientypen spezifischen Aufgaben ab:

- Erstellen eines Richtlinientypobjekts
- Ändern eines vorhandenen Richtlinientypobjekts
- Verwenden von Richtlinientypcontainern
- Exportieren eines Richtlinientyps
- Importieren eines Richtlinientyps
- Konfigurieren einer Richtlinie eines benutzerdefinierten Typs
- Löschen eines Richtlinientypobjekts

Weitere Informationen über Richtlinientypobjekte und Anweisungen bezüglich der Skripterstellung für Richtlinientypobjekte finden Sie in der Dokumentation zu ActiveRoles Server SDK.

Erstellen eines Richtlinientypobjekts

ActiveRoles Server speichert Richtlinientypobjekte im Container **Richtlinientypen**. Sie können auf diesen Container in der ActiveRoles Server-Konsole zugreifen, indem Sie den Zweig **Configuration/Server Configuration** der Konsolenstruktur erweitern.

Gehen Sie folgendermaßen vor, um ein neues Richtlinientypobjekt zu erstellen:

1. Klicken Sie in der Konsolenstruktur unter **Configuration/Server Configuration/Policy Types** mit der rechten Maustaste auf den Richtlinientypcontainer, in dem Sie ein neues Objekt erstellen möchten, und wählen Sie dann **Neu | Richtlinientyp**.

   *Wenn Sie zum Beispiel ein neues Objekt im Root-Container erstellen möchten, klicken Sie mit der rechten Maustaste auf **Richtlinientypen**.*

2. Geben Sie im Assistenten „Neues Objekt – Richtlinientyp" einen Namen, einen Anzeigenamen und optional eine Beschreibung für das neue Objekt ein.

   Der Anzeigename und die Beschreibung werden auf der Seite zur Auswahl einer Richtlinie in den Assistenten, die für die Konfiguration von Richtlinienobjekten verwendet werden, angezeigt.

3. Klicken Sie auf **Weiter**.
4. Klicken Sie auf **Durchsuchen** und wählen Sie das Skriptmodul, das das Skript enthält, das von den Richtlinien dieses Richtlinientyps ausgeführt wird.

   Das Skriptmodul muss im Container „Configuration/Script Modules" vorhanden sein und ein Richtlinienskript enthalten. Weitere Informationen über Richtlinienskripts finden Sie in der ActiveRoles Server SDK-Dokumentation.

5. Führen Sie im Bereich **Kategorie des Richtlinientyps** eine der folgenden Aktionen durch:
   - Klicken Sie auf **Bereitstellung**, wenn Richtlinien dieses Typs für Richtlinienobjekte der Kategorie „Bereitstellung" vorgesehen sind.
   - Klicken Sie auf **Deprovisionierung**, wenn Richtlinien dieses Typs für Richtlinienobjekte der Kategorie „Deprovisionierung" vorgesehen sind.

   *Die Richtlinientypen, für die die Option **Bereitstellung** ausgewählt ist, werden auf der Seite zur Auswahl einer Richtlinie in dem Assistenten angezeigt, der für die Erstellung eines Bereitstellungsrichtlinienobjekts oder zum Hinzufügen von Richtlinien zu einem vorhandenen Bereitstellungsrichtlinienobjekt verwendet wird. Umgekehrt werden die Richtlinientypen, für die die Option **Deprovisionierung** ausgewählt ist, in dem Assistenten zur Erstellung eines Deprovisionsrichtlinienobjekts oder zum Hinzufügen von Richtlinien zu einem solchen Richtlinienobjekt angezeigt.*

6. Überprüfen Sie im Bereich **Richtlinientyp-Symbol** das Bild, das diesen Richtlinientyp angibt. Um ein anderes Bild auszuwählen, klicken Sie auf **Ändern** und öffnen Sie eine Symboldatei, die das gewünschte Bild enthält.

   Dieses Bild wird neben dem Anzeigenamen des Richtlinientyps auf der Assistentenseite zur Auswahl einer zu konfigurierenden Richtlinie angezeigt, um die Identifizierung und visuelle Unterscheidung dieses Richtlinientyps von anderen Richtlinientypen zu erleichtern.

   *Das Bild wird im Richtlinientypobjekt gespeichert. Im Bereich **Richtlinientyp-Symbol** wird das aktuell verwendete Bild angezeigt. Um wieder das Standardbild zu verwenden, klicken Sie auf **Standardsymbol verwenden**. Wenn die Schaltfläche nicht verfügbar ist, dann wird aktuell das Standardbild verwendet.*

7. Klicken Sie auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um die Erstellung des neuen Richtlinientypobjekts abzuschließen.

Ändern eines vorhandenen Richtlinientypobjekts

Sie können ein vorhandenes Richtlinientypobjekt ändern, indem Sie die allgemeinen Eigenschaften, das Skript, die Kategorie oder das Symbol ändern. Die allgemeinen Eigenschaften umfassen den Namen, den Anzeigenamen und die Beschreibung. Die Richtlinientypobjekte befinden sich unter **Configuration/Server Configuration/Policy Types** in der ActiveRoles Server-Konsole.

Die folgende Tabelle fasst die Änderungen zusammen, die Sie an einem vorhandenen Richtlinientypobjekt vornehmen können, vorausgesetzt, dass Sie das Objekt in der ActiveRoles Server-Konsole gefunden haben.

ÄNDERUNG VON	VORGEHENSWEISE	KOMMENTAR
Name des Objekts	Klicken Sie mit der rechten Maustaste auf das Objekt und klicken Sie dann auf **Umbenennen**.	Der Name wird verwendet, um das Objekt zu identifizieren, und muss für die im selben Richtlinientypcontainer enthaltenen Objekte eindeutig sein.
Anzeigename oder Beschreibung	Klicken Sie mit der rechten Maustaste auf das Objekt, klicken Sie auf „Eigenschaften" und nehmen Sie die erforderlichen Änderungen auf der Registerkarte **Allgemein** vor.	Durch die Änderung des Anzeigenamens oder der Beschreibung ändert sich auch der Richtlinienname bzw. die Richtlinienbeschreibung auf der Seite zur Auswahl einer Richtlinie in den Assistenten zur Verwaltung von Richtlinienobjekten.
Skriptmodul	Klicken Sie mit der rechten Maustaste auf das Objekt, klicken Sie auf **Eigenschaften**, dann auf die Registerkarte **Skript**, anschließend auf **Durchsuchen** und wählen Sie dann das gewünschte Skriptmodul aus.	Sie können das Skript in dem Skriptmodul ändern, das aktuell mit dem Richtlinientypobjekt verbunden ist, anstatt ein anderes Skriptmodul auszuwählen. Um das Skript anzuzeigen oder zu ändern, suchen Sie das Skript Modul in der ActiveRoles Server-Konsolenstruktur unter **Configuration/Script Modules** und wählen es aus. Die Änderung des Skripts beeinflusst alle vorhandenen Richtlinien dieses Richtlinientyps. Wenn Sie eine Richtlinie zu einem Richtlinienobjekt hinzufügen und dann das Skript für das Richtlinientypobjekt ändern, auf dessen Grundlage die Richtlinie erstellt wurde, dann führt die Richtlinie das geänderte Skript aus.
Kategorie des Richtlinientyps	Klicken Sie mit der rechten Maustaste auf das Objekt, klicken Sie auf **Eigenschaften**, dann auf die Registerkarte **Skript** und anschließend entweder auf **Bereitstellung** oder auf **Deprovisionierung**.	Durch die Änderung dieser Option ändert sich auch die Darstellung des entsprechenden Richtlinientyps in den Assistenten zur Verwaltung von Richtlinienobjekten. Wenn zum Beispiel die Option von **Bereitstellung** in **Deprovisionierung** geändert wird, wird der Richtlinientyp nicht mehr im Assistenten zur Konfiguration eines Bereitstellungsrichtlinienobjekts angezeigt; statt dessen wird er im Assistenten zur Konfiguration eines Deprovisionsrichtlinienobjekts angezeigt. Die Änderung der Richtlinientypkategorie hat jedoch keinen Einfluss auf die vorhandenen Richtlinien dieses Richtlinientyps. Wenn zum Beispiel eine Richtlinie zu einem Bereitstellungsrichtlinienobjekt hinzugefügt wird, dann bleibt die Richtlinie in diesem Richtlinienobjekt erhalten, selbst wenn die Richtlinientypkategorie von **Bereitstellung** in **Deprovisionierung** im entsprechenden Richtlinientypobjekt geändert wird.

ÄNDERUNG VON	VORGEHENSWEISE	KOMMENTAR
Richtlinientyp-Symbol	Klicken Sie mit der rechten Maustaste auf das Objekt, klicken Sie auf **Eigenschaften** und dann auf die Registerkarte **Skript** und führen Sie anschließend eine der folgenden Aktionen durch: • Klicken Sie auf **Ändern** und öffnen Sie eine Symboldatei, die das gewünschte Symbol enthält. • Klicken Sie auf **Standardsymbol verwenden**, um wieder das Standardbild zu verwenden,	Durch die Änderung dieser Einstellung ändert sich auch das Bild, das neben dem Anzeigenamen des Richtlinientyps in den Assistenten zur Verwaltung von Richtlinienobjekten auf der Seite angezeigt wird, auf der Sie zur Auswahl einer zu konfigurierenden Richtlinie aufgefordert werden.

Verwenden von Richtlinientypcontainern

Sie können einen Richtlinientypcontainer für die Speicherung zugehöriger Richtlinientypobjekte und anderer Richtlinientypcontainer verwenden.

Container bieten die Möglichkeit einer zusätzlichen Kategorisierung von benutzerdefinierten Richtlinientypen und erleichtern somit das Auffinden und die Auswahl der zu konfigurierenden Richtlinie in den Assistenten zur Verwaltung von Richtlinienobjekten. Wenn Sie also ein Richtlinienobjekt erstellen, werden auf der Assistentenseite, auf der Sie zur Auswahl einer Richtlinie aufgefordert werden, die benutzerdefinierten Richtlinientypen zusammen mit den Containern, in denen sich die entsprechenden Richtlinientypobjekte befinden, angezeigt.

Gehen Sie folgendermaßen vor, um einen neuen Richtlinientypcontainer zu erstellen:

1. Klicken Sie in der Konsolenstruktur unter **Configuration/Server Configuration/Policy Types** mit der rechten Maustaste auf den Richtlinientypcontainer, in dem Sie einen neuen Container erstellen möchten, und wählen Sie dann **Neu | Richtlinientypcontainer**.

   *Wenn Sie zum Beispiel einen neuen Container im Root-Container erstellen möchten, klicken Sie mit der rechten Maustaste auf **Richtlinientyp**.*

2. Geben Sie im Assistenten „Neues Objekt – Richtlinientypcontainer" einen Namen und optional eine Beschreibung für den neuen Container ein.

   Der Name und die Beschreibung werden auf der Seite zur Auswahl einer Richtlinie in den Assistenten, die für die Konfiguration von Richtlinienobjekten verwendet werden, angezeigt.

3. Klicken Sie auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um die Erstellung des neuen Containers abzuschließen.

Exportieren eines Richtlinientyps

Sie können ein Richtlinientypobjekt exportieren, sodass die Definition des Richtlinientyps in einer XML-Datei gespeichert wird, die in eine andere ActiveRoles Server-Umgebung importiert werden kann. Das Exportieren und anschließende Importieren von Richtlinientypobjekten erleichtert die Verbreitung von benutzerdefinierten Richtlinien in anderen Umgebungen.

Gehen Sie folgendermaßen vor, um ein Richtlinientypobjekt zu exportieren:

- Klicken Sie mit der rechten Maustaste auf das Richtlinientypobjekt in der ActiveRoles Server-Konsole, klicken Sie dann auf **Exportieren** und geben Sie eine XML-Datei für die Speicherung der Exportdaten an.

Durch den Export eines Richtlinientypobjekts wird eine XML-Datei erstellt, die sowohl das Objekt an sich als auch das Skriptmodul mit dem Richtlinienskript für diesen Richtlinientyp darstellt. Während eines Imports erstellt ActiveRoles Server das Richtlinientypobjekt und das Skriptmodul auf der Grundlage der Daten in der XML-Datei. Als Ergebnis des Imports wird der Richtlinientyp in der neuen Umgebung repliziert und kann dann auf gleiche Weise wie in der Umgebung, aus der er exportiert wurde, verwendet werden.

Importieren eines Richtlinientyps

Sie können ein Richtlinientypobjekt importieren, das dann das importierte Objekt zu einem Richtlinientypcontainer hinzufügt und Ihnen ermöglicht, die von diesem Objekt definierten Richtlinien zu konfigurieren und zu verwenden. Alle für die Bereitstellung eines Richtlinientyps erforderlichen Daten sind in einer XML-Datei enthalten. Um ein Beispiel für das XML-Dokument anzuzeigen, das einen Richtlinientyp angibt, exportieren Sie ein Richtlinientypobjekt und betrachten dann die gespeicherte XML-Datei.

Gehen Sie folgendermaßen vor, um ein Richtlinientypobjekt zu importieren:

1. Klicken Sie in der ActiveRoles Server-Konsolenstruktur unter **Configuration/Server Configuration/Policy Types** mit der rechten Maustaste auf den Richtlinientypcontainer, in den Sie das Richtlinientypobjekt importieren möchten.
2. Klicken Sie auf **Richtlinientyp importieren** und öffnen Sie dann die XML-Datei, die Sie importieren möchten.

Hierdurch wird ein neues Richtlinientypobjekt im auswählten Container erstellt. Außerdem wird ein neues Skript Modul im Container **Configuration/Script Modules** erstellt und mit dem neu erstellten Richtlinientypobjekt verknüpft.

Konfigurieren einer Richtlinie eines benutzerdefinierten Typs

Wenn ein benutzerdefinierter Richtlinientyp bereitgestellt wurde, kann ein ActiveRoles Server-Administrator eine Richtlinie dieses Typs zu einem Richtlinienobjekt hinzufügen. Dies erfolgt durch Auswahl des Richtlinientyps im Assistenten zur Erstellung eines neuen Richtlinienobjekts oder im Assistenten zum Hinzufügen einer Richtlinie zu einem vorhandenen Richtlinienobjekt auswählen.

Welcher Assistent zu verwenden ist, hängt von der Kategorie des Richtlinientyps ab:

- Für einen Richtlinientyp der Kategorie „Bereitstellung" kann eine Richtlinie dieses Typs nur zu einem Bereitstellungsrichtlinienobjekt hinzugefügt werden.
- Für einen Richtlinientyp der Kategorie „Deprovisionierung" kann eine Richtlinie dieses Typs nur zu einem Deprovisionsrichtlinienobjekt hinzugefügt werden.

Gehen Sie folgendermaßen vor, um eine Richtlinie eines benutzerdefinierten Richtlinientyps zu konfigurieren:

1. Befolgen Sie die Anweisungen im Assistenten zur Erstellung eines neuen Richtlinienobjekts oder im Assistenten zum Hinzufügen einer Richtlinie zu einem vorhandenen Richtlinienobjekt.

   Wenn der Richtlinientyp zum Beispiel aus der Kategorie „Bereitstellung" stammt, können Sie den Assistenten zur Erstellung eines neuen Bereitstellungsrichtlinienobjekts verwenden, der durch Anwendung des Befehls ***Neu | Bereitstellungsrichtlinie*** *auf einen Container unter* ***Configuration/Policies/Administration*** *in der ActiveRoles Server-Konsole geöffnet wird.*

2. Klicken Sie auf der Seite **Zu konfigurierende Richtlinie** im Assistenten auf den gewünschten Richtlinientyp.

   Auf der Seite ***Zu konfigurierende Richtlinie*** *werden die benutzerdefinierten Richtlinientypen zusammen mit den vordefinierten ActiveRoles Server-Richtlinientypen aufgelistet. Jeder benutzerdefinierte Richtlinientyp wird durch den Anzeigenamen des entsprechenden Richtlinientypobjekts identifiziert.*

   Die benutzerdefinierten Richtlinientypen sind in einer baumähnlichen Struktur zusammengefasst, die die vorhandene Hierarchie der Richtlinientypcontainer widerspiegelt. Wenn zum Beispiel ein Richtlinientypcontainer erstellt wird, um ein bestimmtes Richtlinientypobjekt zu speichern, wird der Container auch auf der Assistentenseite angezeigt, sodass Sie den Container erweitern müssen, um den Richtlinientyp anzuzeigen oder auszuwählen.

3. Legen Sie auf der Seite **Richtlinienparameter** Parameterwerte für die Richtlinie fest: Klicken Sie auf den Namen eines Parameters in der Liste und klicken Sie dann auf **Bearbeiten**.

   Parameter kontrollieren das Verhalten der Richtlinie. Wenn ActiveRoles Server die Richtlinie ausführt, gibt es die Parameterwerte an das Richtlinienskript weiter. Die vom Skript durchgeführten Vorgänge und die Ergebnisse dieser Vorgänge hängen von den Parameterwerten ab.

   Durch Anklicken von ***Bearbeiten*** *wird eine Seite angezeigt, auf der Sie einen oder mehrere Werte für den ausgewählten Parameter hinzufügen, entfernen oder auswählen können. Für jeden Parameter definiert das Richtlinienskript den Namen des Parameters und andere Merkmale wie etwa eine Beschreibung, eine Liste der akzeptablen Werte, den Standardwert und ob ein Wert erforderlich ist. Wenn eine Liste der akzeptablen Werte definiert ist, dann können Sie nur Werte aus dieser Liste auswählen.*

4. Folgen Sie den Anweisungen des Assistenten, um den Assistenten abzuschließen.

Löschen eines Richtlinientypobjekts

Sie können ein Richtlinientypobjekt löschen, wenn Sie keine Richtlinien des von diesem Objekt angegebenen Typs mehr hinzufügen müssen.

Beachten Sie vor dem Löschen eines Richtlinientypobjekts die folgenden Hinweise:

- Sie können ein Richtlinientypobjekt nur dann löschen, wenn keine Richtlinien des entsprechenden Richtlinientyps in irgendeinem Richtlinienobjekt vorhanden sind. Prüfen Sie jedes Richtlinienobjekt und entfernen Sie die Richtlinien dieses Typs (falls vorhanden) aus dem Richtlinienobjekt, bevor Sie das Richtlinientypobjekt löschen.
- Durch das Löschen eines Richtlinientypobjekts wird dieses dauerhaft aus der ActiveRoles Server-Datenbank gelöscht. Wenn Sie diesen Richtlinientyp erneut verwenden möchten, sollten Sie das Richtlinientypobjekt in eine XML-Datei exportieren, bevor Sie das Objekt löschen.
- Durch das Löschen eines Richtlinientypobjekts wird nicht das mit diesem Objekt verbundene Skriptmodul gelöscht. Das Skriptmodul wird nicht gelöscht, da es möglicherweise von anderen Richtlinien verwendet wird. Wenn das Skriptmodul nicht mehr benötigt wird, kann es separat gelöscht werden.

Gehen Sie folgendermaßen vor, um ein Richtlinientypobjekt zu löschen:

- Klicken Sie mit der rechten Maustaste auf das Richtlinientypobjekt in der ActiveRoles Server-Konsole und klicken Sie dann auf **Löschen**.

6

Bestätigungsprüfung

- Beschreibung der Bestätigungsprüfung
- Konfigurieren der Bestätigungsprüfung
- Starten oder Planen einer Prüfung
- Durchführen der Bestätigung
- Untersuchen der Ergebnisse
- Delegieren von Bestätigungsprüfungsaufgaben

Beschreibung der Bestätigungsprüfung

ActiveRoles Server bietet ein Verfahren für die Durchführung von Prüfungen, die es Managern und anderen verantwortlichen Parteien ermöglichen, die Zugriffsrechte zu überprüfen, die Benutzer aufgrund ihrer Mitgliedschaft in Windows-Gruppen haben. Die periodische Prüfung von Gruppenmitgliedschaftslisten unterstützt die Identifikation und Verwaltung von Benutzerzugriffsrechten, um die Konformität mit Sicherheits- und behördlichen Vorschriften zu gewährleisten. Das Verfahren der Prüfung und Bestätigung der Mitgliedschaft von Gruppen wird als *Bestätigungsprüfung* bezeichnet.

Da Gruppen verwendet werden, um den Zugriff auf Anwendungen und Daten zu kontrollieren, ermöglicht die Implementierung eines Arbeitsablaufs zur Prüfung der Gruppenmitgliedschaft auf regelmäßiger Basis den Organisationen, zuverlässig zu bestätigen, wer Zugriff auf welche Elemente hat – und dies für die gesamte Business- und IT-Umgebung der Organisation. Mit der Bestätigungsprüfungsfunktion ermöglicht ActiveRoles Server den Besitzern von Anwendungen und Daten, den Zugriff auf die Elemente, für die sie verantwortlich sind, direkt zu kontrollieren. Dies reduziert die Last der Rechtfertigung, warum bestimmte Personen Zugriff auf bestimmte Ressourcen haben.

Die Ressourcenbesitzer haben das Business-Know-how, um zu bestimmen, wem ein Zugriff ermöglicht werden kann und wem nicht, und müssen eine Möglichkeit haben, den angemessenen Grad des Benutzerzugriffs auf Ressourcen selbst anzupassen. Die automatisierten Bestätigungsfunktionen von ActiveRoles Server umfassen die Anzeige von Gruppenmitgliedschaftsdaten für die Ressourcenbesitzer, um die Genauigkeit der Daten zu bestätigen und um die Ressourcenbesitzer zu ermächtigen, Fehler zu korrigieren. Die Last der Rechtfertigung der Zugriffsrechte einer bestimmten Person wird so von den Mitarbeitern der IT-Abteilung an die Ressourcenbesitzer übertragen. Neben der Verringerung der Last für die IT-Abteilung durch die Verteilung der Verwaltung auf die Gruppen trägt diese Funktion außerdem dazu bei, dass die Organisationen viele Konformitätsanforderungen erfüllen, die fordern, dass der Ressourcenbesitzer den Zugriff auf die Ressource persönlich kontrolliert.

Nachfolgend sind die wichtigsten Elemente der Funktion „Bestätigungsprüfung" aufgeführt:

- **Schrittweise Konfiguration der Bestätigungsprozesse** Ein Administrator definiert die Zusammenstellung der zu überprüfenden Gruppen und konfiguriert andere Optionen wie etwa die Zeitplan- und Benachrichtigungseinstellungen. Es können mehrere Konfigurationen mit Hilfe der ActiveRoles Server-Konsole erstellt und verwaltet werden.
- **Flexible Definition, welche Gruppen Gegenstand der Prüfung sind** Eine Zusammenstellung von Gruppen kann sowohl mit Hilfe statischer als auch dynamischer Methoden definiert werden. Dynamische Methoden legen Regeln für die Aufnahme oder den Ausschluss von Gruppen in die bzw. aus der Zusammenstellung fest, die auf bestimmten Eigenschaften der Gruppen basieren. Statische Methoden definieren unveränderbare Listen von Gruppen, die in die Zusammenstellung aufgenommen oder aus ihr ausgeschlossen werden sollen.
- **Möglichkeit zum Starten von Prüfungen auf geplanter oder auf Ad-hoc-Basis** Ein Administrator legt das Datum und die Uhrzeit, wann die Bestätigungsprüfung gestartet werden soll, sowie die Anzahl von Tagen, bis wann die Bestätigungsprüfung abgeschlossen sein muss, fest. Eine Prüfung kann so geplant werden, dass sie an einem bestimmten Tag des Monats und in bestimmten Monaten oder nur einmal an einem bestimmten Datum gestartet wird. Ein Administrator kann unabhängig vom vorhandenen Zeitplan eine Ad-hoc-Prüfung starten.
- **Unterstützung von mehreren Prüfungen gleichzeitig** Es können mehrere Prüfungen gleichzeitig ausgeführt werden, ganz gleich, ob auf geplanter Basis oder als Ad-hoc-Prüfung. Dies ermöglicht, dass Prüfungen, die auf verschiedenen Konfigurationen basieren, gleichzeitig ablaufen können.

- **Benachrichtigungen bezüglich bestätigungsrelevanter Ereignisse** ActiveRoles Server bietet E-Mail-Benachrichtigungen in Verbindung mit verschiedenen Ereignissen wie etwa dem Start einer Prüfung an. Folglich können die Verwalter von Gruppen (Gruppenbesitzer) darüber informiert oder daran erinnert werden, dass sie eine Prüfung der Gruppen, für die sie verantwortlich sind, durchführen müssen.
- **Web-Konsole für die Durchführung von Prüfungen** Die Verwalter (Besitzer) der Gruppen verwenden das ActiveRoles Server Web-Interface für die Durchführung der Prüfung. Jedem Verwalter werden nur die Gruppen angezeigt, für die er verantwortlich ist. Der Verwalter kann die Listen der Gruppenmitglieder bei Bedarf anzeigen oder ändern und Gruppen bestätigen.
- **Operationale Berichte über laufende Prüfungen** Für eine laufende Prüfung wird ein Bericht generiert, der die bestätigten sowie nicht bestätigten Gruppen angibt und die Anzeige der Gruppenmitglieder zum Zeitpunkt der Prüfung ermöglicht.
- **Historische Berichte über abgeschlossene Prüfungen** Die für die abgeschlossenen Prüfungen spezifischen Daten werden für Überwachungszwecke archiviert und gespeichert. Berichte über diese Daten bieten den Administratoren oder Prüfern die Möglichkeit, die Gruppen anzuzeigen, die geprüft und bestätigt wurden. Außerdem zeigen sie die Mitgliedschaftslisten der Gruppen zum Zeitpunkt der Bestätigung an.

Die Bereitstellung der automatisierten Bestätigungslösung bietet Organisationen viele Vorteile im Hinblick auf die Zeit- und Kosteneinsparung. Die Automatisierung des Prozesses der Bestätigung von Gruppenmitgliedschaftsdaten stellt eine Möglichkeit dar, Revisionsprüfungen zu beschleunigen, was die fristgerechte Erfüllung von behördlichen Anforderungen erleichtert.

Es kann geplant werden, die Bestätigungsprüfung in regelmäßigen Intervallen wie zum Beispiel jedes Vierteljahr durchzuführen, um die ordnungsgemäße Mitgliedschaft bestimmter Gruppen zu gewährleisten. Die Bestätigungsprüfung ist ein Verfahren, bei dem bestätigt wird, dass jede Gruppe in einer bestimmten Zusammenstellung von Gruppen die folgenden Voraussetzungen erfüllt:

- Die Mitgliedschaftsliste der Gruppe ist vollständig und richtig.
- Die benannten Gruppenmitglieder erfordern von der Gruppe selbst eingeräumte Zugriffsrechte, um ihre Verantwortlichkeiten zu erfüllen.

Die Zusammenstellung von Gruppen erfolgt durch Konfiguration der Bestätigungsprüfung. Es können mehrere Bestätigungsprüfungskonfigurationen erstellt und ausgeführt werden, wobei jede Konfiguration über eine individuelle Zusammenstellung von zu prüfenden und zu bestätigenden Gruppen verfügt.

Die Durchführung der Bestätigungsprüfung umfasst die folgenden Aktivitäten:

- **Konfigurieren der Bestätigungsprüfung** Ein Administrator definiert die Zusammenstellung der zu überprüfenden Gruppen und konfiguriert andere Optionen wie etwa die Zeitplan- und Benachrichtigungseinstellungen. Es können mehrere Konfigurationen mit Hilfe der ActiveRoles Server-Konsole erstellt und verwaltet werden.
- **Starten oder Planen einer Prüfung** Eine Konfiguration kann direkt ausgeführt werden; die Ausführung kann jedoch auch zeitlich geplant werden. Wenn die Konfiguration ausgeführt wird, erstellt sie eine Instanz der Bestätigungsprüfung, wobei die Start- und Enddaten festgelegt sind. Die Prüfung muss während des Zeitraums zwischen dem Startdatum und dem Enddatum durchgeführt werden.

- **Durchführen der Bestätigung** Die Verwalter (Besitzer) der Gruppen verwenden das ActiveRoles Server Web-Interface für die Durchführung der Bestätigungsprüfung. Besitzer werden Gruppen mit Hilfe von Gruppeneigenschaften wie etwa der Eigenschaft „Verwaltet von" zugeordnet und können auf der Seite **Verwaltet von** für ein Gruppenobjekt in der ActiveRoles Server-Konsole oder im Web-Interface verwaltet werden. Jeder Person werden nur die Gruppen angezeigt, denen diese Person als Besitzer zugeordnet wurde. Gruppenbesitzer können die Liste der Gruppenmitglieder anzeigen und, falls erforderlich, ändern sowie Gruppen bestätigen.
- **Untersuchen der Ergebnisse** Die Konfiguration der Bestätigungsprüfung bietet einen konfigurationsspezifischen Bericht über die Instanzen der Bestätigungsprüfung. Der Bericht gibt die bestätigten sowie nicht bestätigten Gruppen an und ermöglicht die Anzeige der Gruppenmitglieder zum Zeitpunkt der Prüfung.

Konfigurieren der Bestätigungsprüfung

Um eine Bestätigungsprüfung durchführen zu können, müssen Sie zunächst mindestens eine Konfiguration erstellen. Die Konfigurationseinstellungen der Bestätigungsprüfung umfassen Folgendes:

- **Name und Beschreibung** Dies ist der Name und die Beschreibung des Objekts, in dem die Konfiguration gespeichert ist. Der Name wird auch verwendet, um die Konfiguration in Bestätigungsprüfungsberichten zu identifizieren.
- **Bestätigende Instanzen** Diese Einstellung gibt an, wer für die Durchführung der Bestätigungsprüfung autorisiert ist. Hierbei kann es sich um die primären Besitzer (Verwalter) oder sekundäre Besitzer der zu überprüfenden Gruppen handeln. Der primäre Besitzer einer Gruppe wird durch die Eigenschaft „Verwaltet von" dieser Gruppe angegeben. Die anderen Besitzer einer Gruppe werden durch die Eigenschaft „Sekundäre Besitzer" dieser Gruppe angegeben.
- **Inhaber der Rolle „Supervisor"** Dies sind die Benutzer oder Benutzergruppen, die den Fortschritt und die Ergebnisse der Bestätigungsprüfung überwachen. Eine Bestätigungsprüfung kann also so konfiguriert werden, dass die Supervisor Benachrichtigungen über bestimmte Ereignisse empfangen, die im Verlauf der Bestätigungsprüfung eintreten.
- **Startzeit und Dauer** Diese Einstellungen legen das Datum und die Uhrzeit, wann die Bestätigungsprüfung gestartet werden soll, sowie die Anzahl von Tagen, bis wann die Bestätigungsprüfung abgeschlossen sein muss, fest. Die Bestätigungsprüfung kann so geplant werden, dass sie an einem bestimmten Tag des Monats und in bestimmten Monaten oder nur einmal an einem bestimmten Datum gestartet wird.
- **Abhilfe** Diese Einstellung gibt an, ob die Gruppen, die innerhalb der Dauer der Bestätigungsprüfung nicht bestätigt wurden, automatisch deprovisioniert werden sollen oder nicht. Eine weitere Option besteht darin, dass der Supervisor nicht bestätigte Gruppen bei Bedarf deprovisioniert.

  Bei Anwendung auf eine Gruppe bezeichnet „Deprovisionierung" eine Reihe von Änderungen, die vorgenommen werden, um die Verwendung der Gruppe zu vermeiden. Welche Änderungen durchgeführt werden müssen, wird von den Deprovisionierungsrichtlinien bestimmt. Wenn die Bestätigungsprüfung für eine Gruppe nicht innerhalb eines bestimmten Zeitraums abgeschlossen wird, was eine potenzielle Bedrohung darstellt, kann die Gruppendeprovisionierung als Abhilfe verwendet werden.
- **Bestätigungsabkommen** Den Personen, die die Bestätigungsprüfung durchführen, wird der Text des Bestätigungsabkommens angezeigt, wenn sie Gruppen bestätigen. Diese Personen müssen die Bedingungen des Bestätigungsabkommens akzeptieren.

- **Gruppen und Regeln** Diese Einstellungen legen die Zusammenstellung der Gruppen fest, die geprüft werden sollen. Sie können einzelne Gruppen auswählen, die in die Zusammenstellung aufgenommen oder aus ihr ausgeschlossen werden sollen. Sie können auch Regeln für die Aufnahme oder den Ausschluss von Gruppen in die bzw. aus der Zusammenstellung aufstellen, die auf bestimmten Eigenschaften der Gruppen basieren.
- **Benachrichtigung** Diese Einstellungen legen die Benachrichtigungsereignisse und -empfänger, den Inhalt der Benachrichtigungs-E-Mails und den ausgehenden E-Mail-Server für die Benachrichtigungs-E-Mails fest.

Gehen Sie wie nachfolgend beschrieben vor, um eine Konfiguration einer Bestätigungsprüfung mittels der ActiveRoles Server-Konsole zu erstellen.

Gehen Sie folgendermaßen vor, um eine Konfiguration der Bestätigungsprüfung zu erstellen:

1. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration | Policies**.
2. Klicken Sie unter **Policies** mit der rechten Maustaste auf **Attestation Review** und wählen Sie **Neu | Bestätigungsprüfungsrichtlinie**.
3. Geben Sie auf der Seite **Übersicht** einen entsprechenden Namen und optional eine Beschreibung für die Konfiguration der Bestätigungsprüfung ein.
4. Klicken Sie auf **Allgemein**.
5. Aktivieren Sie unter **Bestätigende Instanz** eines oder beide dieser Kontrollkästchen:
   - **Primärer Besitzer (Verwalter) einer Gruppe ist autorisiert, diese Gruppe zu bestätigen** Gibt an, dass von den Verwaltern der Gruppen die Durchführung der Bestätigungsprüfung erwartet wird.
   - **Sekundäre Besitzer einer Gruppe sind autorisiert, diese Gruppe zu bestätigen** Gibt an, dass von den anderen Besitzern der Gruppen die Durchführung der Bestätigungsprüfung erwartet wird.

   Die Besitzer einer Gruppe werden auf der Seite **Verwaltet von** für diese Gruppe in der ActiveRoles Server-Konsole oder im Web-Interface angegeben. Der Name des primären Besitzers (Verwalters) wird oben auf der Seite angezeigt. Die sekundären Besitzer werden unten auf der Seite aufgelistet.

   Bei mehreren Besitzern ist die Bestätigungsprüfung für eine Gruppe abgeschlossen, sobald einer der Besitzer diese Gruppe bestätigt hat.
6. Klicken Sie unter **Supervisor** auf **Hinzufügen** und wählen Sie die Benutzer oder Gruppen aus, denen die Rolle des Supervisors zugeordnet werden soll.
7. Wählen Sie unter **Sanierung**, wie Sie die Deprovisionierung auf die Gruppen anwenden möchten, die nicht innerhalb der Dauer der Bestätigungsprüfung geprüft und bestätigt wurden:
   - Wählen Sie **Supervisor die Gruppe bei Bedarf deprovisionieren lassen**, wenn Sie möchten, dass der Supervisor solche Gruppen deprovisioniert, indem er den Befehl **Deprovision** auf die Gruppe anwendet.
   - Wählen Sie **Gruppe automatisch deprovisionieren**, wenn Sie möchten, dass ActiveRoles Server solche Gruppen automatisch deprovisioniert.
8. Klicken Sie auf **Gruppen**.
9. Erstellen Sie die Liste **Gruppen und Regeln**.

   In diesem Schritt definieren Sie eine Zusammenstellung von zu überprüfenden Gruppen. Dies ist eine dynamische Zusammenstellung; d.h., dass Sie sowohl statische als auch dynamische Methoden für die Definition der Mitgliedschaft der Zusammenstellung verwenden können.

Sie können Kriterien für die Mitgliedschaft (Mitgliedschaftsregeln) definieren, die auf der Grundlage von Gruppeneigenschaften wie etwa der Eigenschaft, ob der Gruppenname ein bestimmtes Wort enthält, basieren. Die von Ihnen angegebenen Kriterien haben die Form eines LDAP-Filters. Abhängig vom Regeltyp („Nach Abfrage einschließen" oder „Nach Abfrage ausschließen") werden die Gruppen, die den Kriterien entsprechen, in die Zusammenstellung aufgenommen bzw. aus ihr ausgeschlossen, ohne dass Sie speziell jede Gruppe der Zusammenstellung explizit hinzufügen oder entfernen müssen.

Zusätzlich zur Erstellung von Kriterien für die abfragebasierte Mitgliedschaft (ein LDAP-Filter) können Sie einzelne Gruppen aufnehmen oder ausschließen. Sie können Gruppen explizit hinzufügen, die nicht den Kriterien des Filters entsprechen. Sie können Gruppen, die den Kriterien des Filters entsprechen, jedoch nicht in die Zusammenstellung aufgenommen werden sollen, explizit ausschließen.

Für die Gruppen, die den Kriterien von zwei oder mehr Mitgliedschaftsregeln entsprechen, gilt die folgende Prioritätsfolge:

a) Explizit ausschließen

b) Explizit einschließen

c) Nach Abfrage ausschließen

d) Nach Abfrage einschließen

Folglich gewährleistet die Option „Explizit ausschließen", dass bestimmte Gruppen nicht Teil der Zusammenstellung sind, selbst wenn diese Gruppen mittels der Option „Explizit aufnehmen" oder „Nach Abfrage aufnehmen" hinzugefügt werden.

Um Gruppen zur Zusammenstellung hinzuzufügen oder aus ihr zu entfernen, klicken Sie auf **Einschließen** bzw. **Ausschließen** und verwenden das Dialogfeld **Gruppen auswählen oder Regel konfigurieren**, um Ihre Suchkriterien anzugeben. Sie können die Suchkriterien auf exakt die gleiche Weise angeben, wie Sie dies im Dialogfeld **Suchen** tun. Führen Sie dann eine der folgenden Aktionen durch:

- Um eine Mitgliedschaftsregel hinzuzufügen, die auf den von Ihnen angegebenen Suchkriterien basiert, klicken Sie auf **Regel hinzufügen**.
- Um bestimmte Gruppen auszuwählen, klicken Sie auf **Jetzt suchen**, aktivieren dann die Kontrollkästchen in der Suchergebnisliste und klicken Sie anschließend auf **Auswahl hinzufügen**.

10. Klicken Sie auf **Zielgruppen der Bestätigungsprüfung anzeigen**, um eine Vorschau der von Ihnen konfigurierten Zusammenstellung anzuzeigen. Überprüfen Sie, ob für jede Gruppe die Eigenschaft „Verwaltet von" festgelegt ist.

    Bei diesem Schritt sollten Sie sicherstellen, dass jeder Zielgruppe der Bestätigungsprüfung ein Besitzer zugeordnet ist. Wenn von den primären Besitzern die Durchführung der Bestätigungsprüfung erwartet wird, stellen Sie sicher, dass die Eigenschaft „Verwaltet von" für jede Gruppe aktiviert ist. Wenn die sekundären Besitzer die Bestätigungsprüfung durchführen dürfen, stellen Sie sicher, dass ein sekundärer Besitzer für jede Gruppe angegeben ist. Wenn eine Gruppe über keinen Besitzer verfügt, kann die Bestätigungsprüfung für die Gruppe nicht durchgeführt werden, weil die Gruppe niemandem zur Prüfung zugewiesen werden kann.

    Um eine Liste der Gruppen anzuzeigen, die zu der von Ihnen konfigurierten Zusammenstellung gehören, klicken Sie auf **Zielgruppen der Bestätigungsprüfung anzeigen**. Für jede Gruppe zeigt die Liste den Namen der Gruppe an. Wenn eine Gruppe keinen Besitzer hat, wird der Name der Gruppe rot markiert. Sie können weitere Details für eine Gruppe anzeigen, indem Sie die Liste erweitern: Klicken Sie auf das Plus-Zeichen (+) neben dem Namen der Gruppe.

11. Klicken Sie auf **Benachrichtigung**.
12. Erstellen Sie die Liste **Benachrichtigungsereignisse und -empfänger**.

    In diesem Schritt legen Sie Empfänger als Abonnenten der Benachrichtigungen über Bestätigungsprüfungs-relevante Ereignisse fest und konfigurieren die Benachrichtigungs-E-Mails. ActiveRoles Server bietet E-Mail-Benachrichtigungen in Verbindung mit verschiedenen Ereignissen wie etwa dem Start oder Ende der Bestätigungsprüfung an. Folglich können die Gruppenbesitzer darüber informiert oder daran erinnert werden, dass sie eine Prüfung der Gruppen, für die sie verantwortlich sind, durchführen müssen. Inhaber der Rolle „Supervisor" können über die Gruppen benachrichtigt werden, für die kein Besitzer festgelegt wurde und die daher nicht überprüft werden können.

    Sie können Einträge zur Liste der Benachrichtigungsereignisse und -empfänger hinzufügen, ändern oder aus der Liste entfernen. Um einen neuen Eintrag zu erstellen, klicken Sie auf **Hinzufügen**. Um einen vorhandenen Eintrag zu ändern, wählen Sie sie in der Liste aus und klicken Sie dann auf **Bearbeiten**. Verwenden Sie dann das Dialogfeld **Benachrichtigungseinstellungen**, um den Eintrag zu konfigurieren:

    a) Wählen Sie in der Liste der Ereignisse das Ereignis aus, über dessen Eintreffen Sie benachrichtigen möchten.

    b) Geben Sie unter **Benachrichtigungsempfänger** an, wer die Benachrichtigungen über das ausgewählte Ereignis empfangen soll.

    c) Geben Sie unter **Benachrichtigungszustellung** an, ob die Benachrichtigungen periodisch oder auf einer geplanten Basis gesendet werden sollen. Klicken Sie auf **Konfigurieren**, um den Benachrichtigungsplan aufzustellen. Beachten Sie, dass diese Optionen nicht für alle Ereignisse verfügbar sind.

    d) Klicken Sie unter **Benachrichtigung** auf die Schaltfläche, um die E-Mail-Benachrichtigungs-vorlage anzuzeigen oder zu ändern. Hierdurch wird ein Fenster geöffnet, in dem Sie die Vorlage bearbeiten können, um den Inhalt und das Format der Benachrichtigungs-E-Mails anzupassen. Sie können auch eine auf der Basis der Vorlage generierte Benachrichtigung als Vorschau anzeigen. Die Änderungen, die Sie an einer Vorlage vornehmen, werden je Konfiguration angewandt, sodass die Anpassung einer Vorlage für eine bestimmte Konfiguration nicht diese Vorlage für die anderen Konfigurationen beeinflusst.

    e) Klicken Sie auf **OK**, um das Dialogfeld **Benachrichtigungseinstellungen** zu schließen.

13. Geben Sie im Bearbeitungsfeld unter **Web-Interface**-Adresse die Adresse (URL) der ActiveRoles Server Web-Interface-Seite für die Selbsthilfe ein (zum Beispiel: http://<Server>/ARServerSerfService). Klicken Sie optional auf **Test**, um die Adresse zu überprüfen.

    Diese Adresse wird verwendet, um Hyperlinks in den Benachrichtigungsmeldungen zu erstellen, sodass die Benachrichtigungsempfänger leicht auf Web-Interface-Seiten für die Durchführung von Bestätigungsprüfungen zugreifen können.

14. Wählen Sie aus dem Listenfeld unter **E-Mail-Servereinstellungen** einen Listeneintrag aus, um den entsprechenden abgehenden E-Mail-Server für die Benachrichtigungs-E-Mails anzugeben. Klicken Sie auf **Eigenschaften**, um den ausgewählten Eintrag anzuzeigen oder zu ändern.

    Standardmäßig enthält die Liste einen einzelnen Eintrag. Sie können zusätzliche Einträge erstellen, indem Sie neue Objekte im Container **Configuration/Server Configuration/Mail Configuration** in der ActiveRoles Server-Konsole erstellen.

15. Schließen Sie den Bereich **Konfiguration der Bestätigungsprüfung**.

Der Bereich **Konfiguration der Bestätigungsprüfung** wird auch verwendet, um eine vorhandene Bestätigungsprüfungs-Konfiguration anzuzeigen oder zu ändern. Um den Bereich zu öffnen, klicken Sie auf den Befehl **Eigenschaften** im Menü **Aktion** für das entsprechende Konfigurationsobjekt im Container **Attestation Review**.

Sie können die Befehle im Menü **Aktion** für Objekte im Container **Attestation Review** verwenden, um andere Standardvorgänge wie etwa das Umbenennen oder Löschen einer Bestätigungsprüfungs-Konfiguration durchzuführen.

Starten oder Planen einer Prüfung

Wenn Sie eine Bestätigungsprüfungs-Konfiguration erstellt und konfiguriert haben, können Sie Prüfungen auf der Grundlage dieser Konfiguration ausführen. Die folgenden Optionen sind verfügbar:

- Planen einer Prüfung, sodass diese an einem bestimmten Datum startet
- Planen von Prüfungen, sodass diese an einem bestimmten Tag des Monats und an bestimmten Monaten starten
- Starten einer Ad-hoc-Prüfung unabhängig von der vorhandenen Planung

Sie können diese Optionen im Bereich **Konfiguration der Bestätigungsprüfung** auswählen. Öffnen Sie den Bereich mit Hilfe des Befehls **Eigenschaften** für das Konfigurationsobjekt im Container **Attestation Review** und gehen Sie dann wie nachfolgend beschrieben vor.

Gehen Sie folgendermaßen vor, um eine Prüfung zu planen:

1. Klicken Sie im Bereich **Konfiguration der Bestätigungsprüfung** auf **Allgemein**.
2. Klicken Sie im Bereich **Startzeit und Dauer** auf **Angeben**.
3. Wählen Sie einen Ausführungsplan für die Prüfung aus:
   - **Einmalig** Bei Auswahl dieser Option müssen Sie ein Datum und eine Uhrzeit auswählen an dem bzw. zu der die Prüfung gestartet wird. Die Prüfung wird nur einmal ausgeführt.
   - **Monatlich** Bei Auswahl dieser Option müssen Sie den Zeitplan mittels dieser Parameter konfigurieren:
     - **Startzeit** Die Prüfung startet zu diesem Zeitpunkt.
     - **Tag** Die Prüfung startet an diesem Tag im Monat. Wenn Sie zum Beispiel 3 auswählen, startet die Prüfung am 3. Tag des Monats.
     - **Das <***Auftreten***>** <*des Wochentags*> Die Prüfung startet beim Auftreten eines bestimmten Tages im Monat wie etwa dem zweiten Montag oder dem dritten Dienstag eines Monats.
     - **Des ausgewählten Monats oder der ausgewählten Monate** Die Prüfung startet am angegebenen Tag des ausgewählten Monats oder am angegebenen Tag aller ausgewählten Monate.
4. Geben Sie die Dauer der Prüfung an.

   Die Anzahl der von Ihnen angegebenen Tage bestimmt, wie lange die Prüfung aktiv ist, sodass die Prüfer Vorgänge an den Gruppen, die sie bestätigen sollen, ausführen können.
5. Klicken Sie auf **OK**.

Nachdem Sie die oben aufgeführten Schritte abgeschlossen haben, startet die Bestätigungsprüfung wie durch den Ausführungszeitplan, den Sie in Schritt 3 ausgewählt haben, festgelegt. Sie endet nach Ablauf der Dauer, die Sie in Schritt 4 festgelegt haben. Für eine laufende Bestätigungsprüfung kann die Dauer bei Bedarf verlängert werden (siehe „Durchführen der Bestätigung" weiter unten in diesem Kapitel).

Eine Prüfung kann auch unabhängig vom Zeitplan jederzeit gestartet werden.

Gehen Sie folgendermaßen vor, um eine Ad-hoc-Prüfung zu starten:

1. Klicken Sie im Bereich **Konfiguration der Bestätigungsprüfung** auf **Zusammenfassung**.
2. Klicken Sie auf **Jetzt ausführen**.
3. Geben Sie die Dauer der Prüfung an.
4. Klicken Sie auf **OK**.

Diese Schritte führen zum sofortigen Start der Bestätigungsprüfung; sie ist so viele Tage gültig, wie Sie in Schritt 3 angegeben haben.

Es können mehrere Konfigurationen der Bestätigungsprüfung gleichzeitig ausgeführt werden, ganz gleich, ob auf geplanter Basis oder als Ad-hoc-Prüfung. Dies ermöglicht, dass Prüfungen, die auf verschiedenen Konfigurationen basieren, gleichzeitig ablaufen können.

Durchführen der Bestätigung

Wenn die Bestätigungsprüfung ausgeführt wird, erstellt ActiveRoles Server eine entsprechende Bestätigungsprüfungsinstanz. Dann identifiziert sie die Zusammenstellung der Zielgruppen für diese Instanz der Bestätigungsprüfung und den Prüfer für jede dieser Zielgruppen. Die Besitzer einer Gruppe werden der Aufgabe „Prüfung und Bestätigung der Gruppe" zugewiesen.

Die Prüfer verwenden den Bereich **Eigene Überprüfungen** im ActiveRoles Server Web-Interface, um die Bestätigung der Gruppen durchzuführen. Jedem Prüfer werden nur die Gruppen angezeigt, denen der Prüfer als Besitzer zugeordnet wurde. Weitere Informationen und Anleitungen bezüglich der Verwendung des Web-Interface für die Durchführung von Bestätigungsprüfungen finden Sie im Kapitel „Verwenden von Self-Service Manager" im *ActiveRoles Server Web-Interface – Benutzerhandbuch*.

Die festgelegten Personen wie etwa die Inhaber der Rolle „Bestätigungsprüfungs-Supervisor" können die ActiveRoles Server-Konsole verwenden, um die laufende Prüfung zu überwachen – d. h. die Bestätigungsprüfungsinstanz, die derzeit ausgeführt wird. Insbesondere können Sie folgende Aktionen ausführen:

- Prüfen der aktuellen Ergebnisse der laufenden Prüfung
- Verlängern der Dauer der laufenden Prüfung
- Stoppen der laufenden Prüfung

Die mit der Verwaltung einer laufenden Prüfung verbundenen Aufgaben werden ausgehend vom Bereich **Konfiguration der Bestätigungsprüfung** durchgeführt. Öffnen Sie den Bereich mit Hilfe des Befehls **Eigenschaften** für das Bestätigungsprüfungs-Konfigurationsobjekt im Container **Attestation Review** und gehen Sie dann wie nachfolgend beschrieben vor.

Gehen Sie folgendermaßen vor, um die aktuellen Ergebnisse der laufenden Prüfung zu untersuchen:

- Klicken Sie auf der Seite **Zusammenfassung** im Bereich **Konfiguration der Bestätigungsprüfung** auf **Ergebnisse der Prüfung anzeigen**.

  Diese Schaltfläche wird nur angezeigt, während die Prüfung läuft.

Hierdurch wird ein Bericht angezeigt, in dem die Zielgruppen der Bestätigungsprüfung aufgeführt sind. Der Bericht gibt für jede Gruppe an, ob die Gruppe vom angegebenen Prüfer bestätigt wurde. Außerdem zeigt er die Mitgliedschaftsliste der Gruppe an. Ausführlichere Informationen finden Sie unter „Untersuchen der Ergebnisse" weiter unten in diesem Kapitel.

Gehen Sie folgendermaßen vor, um die Dauer der laufenden Prüfung zu verlängern:

1. Klicken Sie auf der Seite **Zusammenfassung** im Bereich **Konfiguration der Bestätigungsprüfung** auf **Prüfung verlängern**.

   Diese Schaltfläche wird nur angezeigt, während die Prüfung läuft.

2. Geben Sie die neue Dauer für die Prüfung an und klicken Sie dann auf **OK**.

Von den Prüfern wird erwartet, die Prüfung bis zum Ablauf der Gültigkeitsdauer der Bestätigungsprüfung abzuschließen und die Gruppen zu bestätigen. Die Gültigkeitsdauer beginnt mit dem Tag, an dem die Bestätigungsprüfung gestartet wird, und endet nach der angegebenen Anzahl von Tagen nach dem Start.

Gehen Sie folgendermaßen vor, um die laufende Prüfung zu stoppen:

- Klicken Sie auf der Seite **Zusammenfassung** im Bereich **Konfiguration der Bestätigungsprüfung** auf **Prüfung stoppen**.

  Diese Schaltfläche wird nur angezeigt, während die Prüfung läuft.

Wenn eine Prüfung gestoppt wird, können die Prüfer die an der Prüfung beteiligten Gruppen nicht mehr bestätigen. Wenn eine Prüfung gestoppt wird, werden jedoch nicht die prüfungsspezifischen Prüfungsdaten gelöscht. Die Informationen über die Prüfung einschließlich des bestätigungsrelevanten Status der Zielgruppen werden von ActiveRoles Server gespeichert und können in den von der Konsole bereitgestellten Prüfungsberichten eingesehen werden. Ausführlichere Informationen finden Sie unter „Untersuchen der Ergebnisse" weiter unten in diesem Kapitel.

Untersuchen der Ergebnisse

Bei Ausführung einer bestimmten Konfiguration der Bestätigungsprüfung generiert ActiveRoles Server eine auf dieser Konfiguration basierende Bestätigungsprüfungsinstanz und versetzt die Instanz in einen aktiven Status. Die Instanz ist während der angegebenen Dauer der Prüfung aktiv. Wenn die Prüfungsdauer abgelaufen ist oder wenn die Prüfung manuell gestoppt wird, wird die Instanz in den inaktiven Status versetzt. Das instanzspezifische Prüfungsdatum wird für Überwachungszwecke gespeichert. Diese Überwachungsdaten bilden eine historische Instanz der Bestätigungsprüfung.

Eine Konfiguration kann jeweils nur über eine aktive Instanz verfügen. Darüber hinaus hat eine Konfiguration normalerweise eine Reihe von historischen Instanzen, die den Audit Trail der Prüfungen darstellen, die auf der Grundlage dieser Konfiguration durchgeführt wurden. Jede historische Instanz ist durch den Namen der Konfiguration und das Startdatum der Prüfung gekennzeichnet. Die ActiveRoles Server-Konsole ermöglicht Ihnen, sowohl aktive als auch historische Instanzen zu überprüfen.

Untersuchen der Ergebnisse einer laufenden Prüfung

Während eine Konfiguration ausgeführt wird, befindet sich die entsprechende Bestätigungsprüfungs-instanz in einem aktiven Status, was die laufende Prüfung angibt. Der Fortschritt und die Ergebnisse einer laufenden Prüfung können ausgehend vom Bereich **Konfiguration der Bestätigungsprüfung** untersucht werden.

Gehen Sie folgendermaßen vor, um die aktuellen Ergebnisse einer laufenden Prüfung zu untersuchen:

1. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration | Policies** und wählen Sie den Container **Attestation Review**.
2. Wählen Sie im Container **Attestation Review** die Konfiguration der Bestätigungsprüfung aus, auf der die laufende Prüfung basiert.

   Die Prüfung, die Sie untersuchen werden, wurde unter Verwendung einer bestimmten Konfiguration gestartet. Um auf die *Ergebnisse der Prüfung zuzugreifen, müssen Sie den Bereich* ***Konfiguration der Bestätigungsprüfung*** *für diese Konfiguration öffnen.*
3. Klicken Sie mit der rechten Maustaste auf das Objekt, das die Konfiguration der Bestätigungsprüfung angibt, und klicken Sie dann auf **Eigenschaften**, um den Bereich **Konfiguration der Bestätigungsprüfung** zu öffnen.
4. Klicken Sie auf der Seite **Zusammenfassung** auf **Ergebnisse der Prüfung anzeigen**.

   Diese Schaltfläche wird nur angezeigt, während die Prüfung läuft.

Hierdurch wird ein Bericht angezeigt, in dem die Zielgruppen der Prüfung aufgeführt sind. Der Bericht gibt für jede Gruppe an, ob die Gruppe von einem Prüfer bestätigt wurde. Außerdem zeigt er die Mitgliedschaftsliste der Gruppe an.

Die vom Bericht generierte Gruppenliste umfasst die folgenden Felder:

- **Gruppe** Name der Gruppe.
- **Bestätigt** Gibt an, ob der Prüfer die Gruppe bestätigt hat oder nicht.
- **Primärer Besitzer (Verwalter)** Gibt das in der Eigenschaft „Verwaltet von" der Gruppe festgelegte Konto an; ob der primäre Besitzer als ein Prüfer agieren kann, hängt von der Konfiguration der Bestätigungsprüfung ab.
- **Sekundäre Besitzer** Gibt die in der Eigenschaft „Sekundäre Besitzer" der Gruppe festgelegten Konten an; ob die sekundären Besitzer als Prüfer agieren können, hängt von der Konfiguration der Bestätigungsprüfung ab.

Sie können weitere Details für eine Gruppe anzeigen, indem Sie die Liste erweitern: Klicken Sie auf das Plus-Zeichen (+) neben dem Namen der Gruppe. Die Liste kann erweitert werden: Klicken Sie auf das Plus-Zeichen (+) in der Überschrift **Mitglieder**, um die Mitgliedschaftsliste der Gruppe anzuzeigen.

Wenn eine Gruppe als bestätigt markiert ist, zeigt der Bericht die Gruppenmitgliedschaftsliste, so wie diese zu dem Zeitpunkt, an dem die Gruppe bestätigt wurde, Bestand hatte.

Das Fenster, in dem der Bericht angezeigt wird, erfüllt auch einige häufige Berichterstattungsanfor-derungen einschließlich der Möglichkeit, alle gemeldeten Ergebnisse zum Drucken oder Anzeigen in einer Datei zu dokumentieren. Mit dem Kontextmenü können Sie den Bericht in eine Datei im HTML- oder XML-Format exportieren, ihn drucken oder über E-Mail versenden.

Untersuchen von historischen Ergebnissen

Jede der historischen Instanzen der Bestätigungsprüfung stellt eine abgeschlossene Prüfung dar, die auf der Grundlage einer bestimmten Konfiguration durchgeführt wurde. Die historischen Ergebnisse einer abgeschlossenen Prüfung können ausgehend vom Bereich **Konfiguration der Bestätigungsprüfung** untersucht werden.

Gehen Sie folgendermaßen vor, um die historischen Ergebnisse einer abgeschlossenen Prüfung zu untersuchen:

1. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration | Policies** und wählen Sie den Container **Attestation Review**.
2. Wählen Sie im Container **Attestation Review** die Konfiguration der Bestätigungsprüfung aus, die für die Durchführung der Prüfung verwendet wurde.

   Die Prüfung, die Sie untersuchen werden, wurde unter Verwendung einer bestimmten Konfiguration durchgeführt. Um auf die *Ergebnisse der Prüfung zuzugreifen, müssen Sie den Bereich* ***Konfiguration der Bestätigungsprüfung*** *für diese Konfiguration öffnen.*
3. Klicken Sie mit der rechten Maustaste auf das Objekt, das die Konfiguration der Bestätigungsprüfung angibt, und klicken Sie dann auf **Eigenschaften**, um den Bereich **Konfiguration der Bestätigungsprüfung** zu öffnen.
4. Klicken Sie auf der Seite **Zusammenfassung** auf **Historische Ergebnisse der Bestätigungsprüfung anzeigen**.
5. Klicken Sie im linken Bereich des Fensters **Ergebnisse der Bestätigungsprüfung** auf das Startdatum einer Prüfung, um die Details für diese Prüfung anzuzeigen.

Hierdurch wird ein Bericht angezeigt, in dem die Zielgruppen der Prüfung aufgeführt sind. Der Bericht gibt für jede Gruppe an, ob die Gruppe von einem Prüfer bestätigt wurde. Außerdem zeigt er die Mitgliedschaftsliste der Gruppe an.

Standardmäßig umfasst die vom Bericht generierte Gruppenliste die folgenden Felder:

- **Gruppe** Name der Gruppe.
- **Bestätigt** Gibt an, ob die Gruppe bestätigt wurde oder nicht.
- **Primärer Besitzer (Verwalter)** Gibt das in der Eigenschaft „Verwaltet von" der Gruppe festgelegte Konto an; ob der primäre Besitzer als ein Prüfer agieren kann, hängt von der Konfiguration der Bestätigungsprüfung ab.
- **Sekundäre Besitzer** Gibt die in der Eigenschaft „Sekundäre Besitzer" der Gruppe festgelegten Konten an; ob die sekundären Besitzer als Prüfer agieren können, hängt von der Konfiguration der Bestätigungsprüfung ab.

Sie können weitere Details für eine Gruppe anzeigen, indem Sie die Liste erweitern: Klicken Sie auf das Plus-Zeichen (+) neben dem Namen der Gruppe. Die Liste kann erweitert werden: Klicken Sie auf das Plus-Zeichen (+) in der Überschrift **Mitglieder**, um die Mitgliedschaftsliste der Gruppe anzuzeigen.

Wenn eine Gruppe als bestätigt markiert ist, zeigt der Bericht die Gruppenmitgliedschaftsliste, so wie diese zu dem Zeitpunkt, an dem die Gruppe bestätigt wurde, Bestand hatte.

Delegieren von Bestätigungsprüfungsaufgaben

ActiveRoles Server bietet eine Reihe von Zugriffsvorlagen, die es dem Administrator ermöglichen, die folgenden, im Zusammenhang mit der Bestätigungsprüfung stehenden Aufgaben zu delegieren:

- **Bestätigungsprüfung konfigurieren** Dies impliziert den Vollzugriff auf die Konfiguration der Bestätigungsprüfung einschließlich der Möglichkeit zum Erstellen neuer Konfigurationen und zur Ausführung vorhandener Konfigurationen ausgehend von der ActiveRoles Server-Konsole.
- **Prüfung durchführen** Diese Option bezieht sich auf die Möglichkeit für die Verwalter der Gruppen, die Gruppenmitgliedschaft im Bereich **Eigene Überprüfungen** des ActiveRoles Server Web-Interface zu überprüfen und zu bestätigen.
- **Ergebnisse überprüfen** Diese Option setzt einen schreibgeschützten Zugriff auf Bestätigungsprüfungskonfigurationen einschließlich der Möglichkeit, Berichte über laufende und abgeschlossene Prüfungen anzuzeigen, voraus.

Die nachfolgend aufgeführten Unterabschnitte enthalten Anweisungen bezüglich der Delegation jeder dieser Aufgaben an normale Benutzer oder Gruppen, die nicht über Administratorrechte für ActiveRoles Server verfügen.

Ermöglichen der Anzeige des Containers „Attestation Review" für Benutzer oder Gruppen

Wenn irgendeine der Bestätigungsprüfungsaufgaben erfordert, dass die Benutzer oder Gruppen, die die Aufgabe ausführen, auf den Container **Attestation Review** in der ActiveRoles Server-Konsole zugreifen können, dann muss der Administrator die entsprechende Zugriffsvorlage (siehe unten) anwenden, um diesen Benutzern oder Gruppen die Anzeige dieses Containers in der Konsolenstruktur zu ermöglichen.

Gehen Sie folgendermaßen vor, um die Anzeige des Containers „Attestation Review" für Benutzer oder Gruppen zu ermöglichen:

1. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf **Configuration** und klicken Sie dann auf **Kontrolle delegieren**.
2. Klicken Sie im Dialogfeld **ActiveRoles Server-Sicherheit** auf **Hinzufügen**, um den Assistenten zum Delegieren der Kontrolle zu starten.
3. Klicken Sie auf der Seite **Benutzer oder Gruppen** im Assistenten auf **Hinzufügen** und verwenden Sie dann das Dialogfeld **Objekte auswählen**, um die Benutzer oder Gruppen auszuwählen, denen Sie die Befugnis für die Ausführung der Aufgabe erteilen möchten.
4. Klicken Sie auf der Seite **Zugriffsvorlagen** im Assistenten auf das Plus-Zeichen (+) neben dem Ordner **Bestätigungsprüfung** unter **Zugriffsvorlagen** und aktivieren Sie das Kontrollkästchen neben der Bezeichnung **Attestation Review – View Attestation Review Container**.
5. Befolgen Sie die Anweisungen des Assistenten und übernehmen Sie die Standardeinstellungen.
6. Klicken Sie im Dialogfeld **ActiveRoles Server-Sicherheit** auf **OK**.

Delegieren des Vollzugriffs auf alle Bestätigungsprüfungskonfigurationen

Durch die Erteilung eines Vollzugriffs auf alle Bestätigungsprüfungskonfigurationen an einen Benutzer oder eine Gruppe erteilen Sie diesem Benutzer oder dieser Gruppe die Befugnis zur Durchführung der folgenden Aufgaben:

- Erstellen von neuen Konfigurationen
- Vornehmen von Änderungen an vorhandenen Konfigurationen
- Starten, Planen, Verlängern oder Stoppen von Prüfungen auf der Grundlage einer beliebigen Konfiguration
- Anzeigen spezifischer Berichte für jede Konfiguration

Delegieren des Vollzugriffs auf alle Konfigurationen:

- Wiederholen Sie die im Abschnitt „Ermöglichen der Anzeige des Containers „Bestätigungsprüfungen" für Benutzer oder Gruppen" aufgeführten Schritte mit den folgenden Änderungen:
  a) Erweitern Sie in Schritt 1 **Configuration | Policies** und klicken Sie mit der rechten Maustaste auf **Attestation Review** unter **Policies**.
  b) Aktivieren Sie in Schritt 4 das Kontrollkästchen neben der Bezeichnung **Attestation Review – Full Control**.

Delegieren des Vollzugrifs auf eine bestimmte Konfiguration der Bestätigungsprüfung

Durch die Erteilung des Vollzugriffs auf eine bestimmte Konfiguration der Bestätigungsprüfung an einen Benutzer oder eine Gruppe autorisieren Sie den Benutzer oder die Gruppe zur Durchführung der folgenden Aufgaben:

- Vornehmen von Änderungen an dieser Konfiguration
- Starten, Planen, Verlängern oder Stoppen von Prüfungen auf der Grundlage dieser Konfiguration
- Anzeigen von für diese Konfiguration spezifischen Berichten

Sie können dem Inhaber der Rolle „Supervisor" für eine bestimmte Konfiguration den Vollzugriff auf diese Konfiguration gewähren.

Delegieren des Vollzugriffs auf eine bestimmte Konfiguration:

- Wiederholen Sie die im Abschnitt „Ermöglichen der Anzeige des Containers „Bestätigungsprüfungen" für Benutzer oder Gruppen" aufgeführten Schritte mit den folgenden Änderungen:
  a) Erweitern Sie in Schritt 1 **Configuration | Policies**, wählen Sie **Attestation Review** unter **Policies** aus, klicken Sie mit der rechten Maustaste auf das Konfigurationsobjekt im Bereich „Details" und klicken Sie dann auf **Objektverwaltung zuweisen**.
  b) Aktivieren Sie in Schritt 4 das Kontrollkästchen neben der Bezeichnung **Attestation Review – Full Control**.

Gewähren eines schreibgeschützten Zugriffs für Benutzer oder Gruppen auf alle Konfigurationen der Bestätigungsprüfung

Indem Sie einem Benutzer oder einer Gruppe einen schreibgeschützten Zugriff auf alle Konfigurationen der Bestätigungsprüfung gewähren, ermöglichen Sie dem Benutzer oder der Gruppe die Anzeige von konfigurationsspezifischen Berichten sowie die Anzeige aller Konfigurationseinstellungen.

Gewähren eines schreibgeschütztem Zugriffs für Benutzer oder Gruppen auf alle Konfigurationen:

- Wiederholen Sie die im Abschnitt „Ermöglichen der Anzeige des Containers „Bestätigungsprüfungen" für Benutzer oder Gruppen" aufgeführten Schritte mit den folgenden Änderungen:
  a) Erweitern Sie in Schritt 1 **Configuration | Policies** und klicken Sie mit der rechten Maustaste auf **Attestation Review** unter **Policies**.
  b) Aktivieren Sie in Schritt 4 das Kontrollkästchen neben der Bezeichnung **Attestation Review – View Reports**.

Gewähren eines schreibgeschützten Zugriffs für Benutzer oder Gruppen auf eine bestimmte Konfiguration der Bestätigungsprüfung

Indem Sie einem Benutzer oder einer Gruppe einen schreibgeschützten Zugriff auf eine bestimmte Konfiguration der Bestätigungsprüfung gewähren, ermöglichen Sie dem Benutzer oder der Gruppe die Anzeige von Berichten und Konfigurationseinstellungen, die spezifisch für diese Konfiguration sind.

Gewähren eines schreibgeschütztem Zugriffs für Benutzer oder Gruppen auf eine bestimmte Konfiguration:

- Wiederholen Sie die im Abschnitt „Ermöglichen der Anzeige des Containers „Bestätigungsprüfungen" für Benutzer oder Gruppen" aufgeführten Schritte mit den folgenden Änderungen:
  a) Erweitern Sie in Schritt 1 **Configuration | Policies**, wählen Sie **Attestation Review** unter **Policies** aus, klicken Sie mit der rechten Maustaste auf das Konfigurationsobjekt im Bereich „Details" und klicken Sie dann auf **Objektverwaltung zuweisen**.
  b) Aktivieren Sie in Schritt 4 das Kontrollkästchen neben der Bezeichnung **Attestation Review – View Reports**.

Autorisieren von Gruppenbesitzern zur Durchführung von Prüfungsaufgaben

Um die Mitgliedschaft von Gruppen überprüfen und bestätigen zu können, müssen den Besitzern (Verwaltern) der Gruppen die entsprechenden Rechte in ActiveRoles Server gewährt werden. Um die Gruppenbesitzer für die Durchführung von Prüfungsaufgaben mit Hilfe des Web-Interface zu autorisieren, müssen Sie die Zugriffsvorlage **Perform Attestation** wie nachfolgend beschrieben anwenden.

Gehen Sie folgendermaßen vor, um Gruppenbesitzer zur Durchführung von Prüfungsaufgaben zu autorisieren:

1. Suchen Sie in der ActiveRoles Server-Konsole den Container, in dem sich die Zielgruppen der Bestätigungsprüfung befinden, klicken Sie mit der rechten Maustaste auf den Container und klicken Sie dann auf **Kontrolle delegieren**.
2. Klicken Sie im Dialogfeld **ActiveRoles Server-Sicherheit** auf **Hinzufügen**, um den Assistenten zum Delegieren der Kontrolle zu starten.
3. Klicken Sie auf der Seite **Benutzer oder Gruppen** im Assistenten auf **Hinzufügen**, um das Dialogfeld **Objekte auswählen** zu öffnen.

4. Geben Sie im Bearbeitungsfeld unter der Schaltfläche **Hinzufügen** im Dialogfeld **Objekte auswählen** eine der folgenden Optionen ein und klicken Sie dann auf **OK**:
   - Geben Sie **ActiveRoles Built-in\Primary Owner (Managed By)** ein, um die Verwalter der Gruppen zur Durchführung von Prüfungsaufgaben zu autorisieren.
   - Geben Sie **ActiveRoles Built-in\Secondary Owners** ein, um andere Besitzer der Gruppen zur Durchführung von Prüfungsaufgaben zu autorisieren.

   *Sie können auch das integrierte Konto **Primärer Besitzer (Verwaltet von)** oder **Sekundäre Besitzer** aus der Liste im Dialogfeld **Objekte auswählen** auswählen.*
5. Klicken Sie auf der Seite **Zugriffsvorlagen** im Assistenten auf das Plus-Zeichen (+) neben dem Ordner **Attestation Review** unter **Access Templates** und aktivieren Sie das Kontrollkästchen neben der Bezeichnung **Attestation Review – Perform Attestation**.
6. Befolgen Sie die Anweisungen des Assistenten und übernehmen Sie die Standardeinstellungen.
7. Klicken Sie im Dialogfeld **ActiveRoles Server-Sicherheit** auf **OK**.

7

Arbeitsabläufe

- Beschreibung der Arbeitsabläufe
- Konfigurieren eines Arbeitsablaufs
- Beispiel: Genehmigungs-Arbeitsablauf

Beschreibung der Arbeitsabläufe

ActiveRoles Server bietet ein umfassendes Arbeitsablaufsystem für die Automatisierung und Integration der Verwaltung von Verzeichnisdaten. Dieses auf der Windows Workflows Foundation-Technologie von Microsoft basierende Arbeitsablaufsystem ermöglicht IT-Spezialisten, Verwaltungsregeln schnell und einfach zu definieren, zu automatisieren und zu erzwingen. Arbeitsabläufe erweitern die Möglichkeiten von ActiveRoles Server, indem Sie einen Rahmen bieten, der die Kombination vielseitiger Verwaltungsregeln wie etwa die Bereitstellung und Deprovisionierung von Identitätsinformationen im Verzeichnis, die Durchsetzung von Richtlinienregeln für Änderungen an den Identitätsdaten, die Weiterleitung von Datenänderungen zu Genehmigungszwecken, E-Mail-Benachrichtigungen über bestimmte Ereignisse und Bedingungen sowie die Möglichkeit zur Implementierung benutzerdefinierter Vorgänge mit Hilfe von Skripttechnologien wie etwa Microsoft Windows PowerShell oder VBScript ermöglicht.

Angenommen, Sie müssen Benutzerkonten auf der Grundlage von Daten aus externen Systemen bereitstellen. Die Daten werden abgerufen und dann mit Hilfe eines Dienstes wie etwa ActiveRoles Quick Connect, das in Verbindung mit ActiveRoles Server arbeitet, an das Verzeichnis weitergeleitet. Für die Koordination der im Zusammenhang mit der Kontobereitstellung stehenden Vorgänge kann ein Arbeitsablauf erstellt werden. So können zum Beispiel verschiedene Regeln für die Erstellung oder Aktualisierung der in verschiedenen Containern befindlichen Konten angewandt werden.

Arbeitsabläufe können auch Genehmigungsregeln enthalten, die erfordern, dass bestimmte Änderungen von zuvor bestimmten Personen (genehmigende Instanzen) autorisiert werden. Beim Entwurf eines Genehmigungs-Arbeitsablaufs gibt der Administrator an, welche Art von Vorgang zum Start des Arbeitsablaufs führt, und fügt Genehmigungsregeln zum Arbeitsablauf hinzu. Die Genehmigungsregeln legen fest, wer autorisiert ist, den Vorgang zu genehmigen. Sie legen außerdem die erforderliche Reihenfolge der Genehmigungen und die Personen, die über Genehmigungsaufgaben oder Entscheidung informiert werden sollen, fest.

Durch das Senden von E-Mail-Benachrichtigungen erweitern Arbeitsabläufe die Reichweite der Verwaltungprozessautomatisierung auf das gesamte Unternehmen. Benachrichtigungsaktivitäten in einem Arbeitsablauf ermöglichen die Benachrichtigung per E-Mail von Personen über Ereignisse, Bedingungen oder Aufgaben, die ihre Aufmerksamkeit erfordern. So können zum Beispiel Genehmigungsregeln über Änderungsanforderungen informieren, die auf eine Genehmigung warten. Es können auch separate Benachrichtigungsregeln angewandt werden, um über Datenänderungen im Verzeichnis zu informieren. Benachrichtigungsmeldungen umfassen alle erforderlichen unterstützenden Informationen und bieten Hyperlinks, die es den Nachrichtenempfängern ermöglichen, Aktionen mittels eines standardmäßigen Webbrowsers zu ergreifen.

Wichtige Funktionsmerkmale und Definitionen

In diesem Abschnitt sind einige wichtige Konzepte zusammengefasst, die für den Entwurf und die Implementierung von Arbeitsabläufen in ActiveRoles Server gelten.

Arbeitsablauf

Ein Arbeitsablauf Befolgen Sie die Anweisungen des Assistenten und übernehmen Sie die beschreibt, der aus Schritten oder Aktivitäten besteht. Arbeitsabläufe beschreiben die Reihenfolge der Ausführung und Beziehungen zwischen Aktivitäten, die für die Durchführung bestimmter Vorgänge erforderlich sind. In ActiveRoles Server stellen Arbeitsabläufe eine Möglichkeit dar, Bereitstellungsvorgänge und die allgemeine Verwaltung von Verzeichnisdaten anzupassen. Arbeitsabläufe können also verwendet werden, um Genehmigungen zu Benutzerbereitstellungsprozesses hinzuzufügen oder die Benutzerbereitstellungsprozesse in externe Systeme zu integrieren.

Arbeitsablaufdefinition

Eine Arbeitsablaufdefinition ist eine Darstellung der Arbeitsablaufstruktur. Die Definition eines Arbeitsablaufs wird als ein einzelnes Objekt im ActiveRoles Server-Konfigurationsdatenspeicher gespeichert und kann als ein XML-Dokument strukturiert sein, dass die Arbeitsablauf-Startbedingungen, die Aktivitäten, die Parameter für die Aktivitäten und die Reihenfolge, in der die Aktivitäten ausgeführt werden sollen, definiert.

Arbeitsablauf-Startbedingungen

Die Arbeitsablaufeinstellungen, die festlegen, welche Vorgänge zum Start des Arbeitsablaufs führen, werden als „Arbeitsablauf-Startbedingungen" bezeichnet. Ein Arbeitsablauf kann zum Beispiel so konfiguriert sein, dass jede Anforderung zur Erstellung eines Benutzerkontos in einem bestimmten Container den Arbeitsablauf startet.

Arbeitsablaufinstanz

Durch den Start eines Arbeitsablaufs wird eine Arbeitsablaufinstanz auf der Grundlage von der Einstellungen in der Arbeitsablaufdefinition erstellt. Jede Arbeitsablaufinstanz speichert die Laufzeitdaten, die den aktuellen Status eines einzelnen, gerade ausgeführten Arbeitsablaufs angeben.

Arbeitsablaufaktivität

Eine Arbeitsablaufaktivität ist eine logisch isolierte Einheit, die einen bestimmten operationalen Schritt eines Arbeitsablaufs implementiert. Die in einer Aktivität enthaltene Logik gilt sowohl während des Entwurfs, wenn Sie die Aktivität zu einer Arbeitsablaufdefinition hinzufügen, als auch bei Ausführung, wenn eine Arbeitsablaufinstanz ausgeführt wird. Wenn die Ausführung alle Aktivitäten in einem bestimmten Flusspfad abgeschlossen ist, ist die Arbeitsablaufinstanz abgeschlossen.

Arbeitsablauf-Designer (Workflow Designer)

Der Workflow Designer ist ein von ActiveRoles Server für die Erstellung von Arbeitsabläufen bereitgestelltes grafisches Tool. Das Tool stellt die Arbeitsablaufdefinition als ein Prozessdiagramm mit Symbolen, die Arbeitsablaufaktivitäten angeben, und direktionalen Pfeilen, die die Übergänge zwischen den Aktivitäten angeben, dar. Benutzer ziehen Aktivitäten vom Aktivitätsbereich auf das Prozessdiagramm und konfigurieren sie mit Hilfe der von der Designer-Schnittstelle bereitgestellten Seiten. Für die Konfiguration der Arbeitsablauf-Startbedingungen stehen separate Seiten zur Verfügung.

Arbeitsablauf-Modul

ActiveRoles Server nutzt das Laufzeitmodul von Microsoft Windows Workflow Foundation für die Erstellung und Pflege von Arbeitsablaufinstanzen. Das Modul unterstützt mehrere, parallel ausgeführte Arbeitsablaufinstanzen. Wenn ein Arbeitsablauf gestartet wird, überwacht das Modul den Status der Arbeitsablaufinstanz, koordiniert die Weiterleitung der Aktivitäten in der Arbeitsablaufinstanz, bestimmt, welche Aktivitäten für die Ausführung ausgewählt werden dürfen, und führt Aktivitäten aus. Das Arbeitsablauf-Modul wird im Prozess mit dem Verwaltungsdienst gehostet, der bei Laufzeit Arbeitsabläufen die Kommunikation mit ActiveRoles Server ermöglicht.

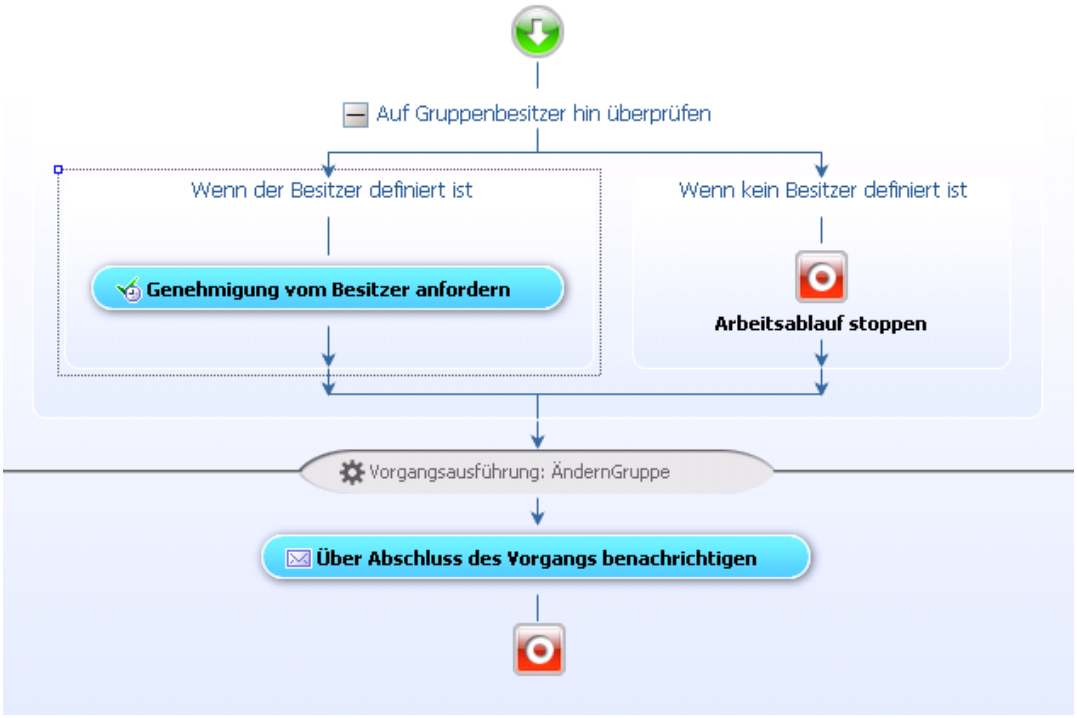
E-Mail-Benachrichtigungen

Benutzer werden per E-Mail über bestimmte, innerhalb eines Arbeitsablaufs eintretende Situation benachrichtigt. Eine Benachrichtigungsmeldung wird generiert und an die angegebenen Empfänger gesendet, um sie über den Eintritt eines bestimmten Ereignisses wie etwa das Senden einer neuen Genehmigungsaufgabe an die genehmigenden Instanzen oder den Abschluss des Vorgangs zu informieren. Eine Benachrichtigungskonfiguration umfasst solche Elemente wie etwa das Ereignis, bei dessen Eintritt eine Benachrichtigung erfolgen soll, die Liste der Benachrichtigungsempfänger und die Vorlage für die Benachrichtigungsmeldung.

Arbeitsablaufprozesse

Die Logik eines automatisierten Verwaltungsprozesses kann mit Hilfe von administrativen Richtlinien in ActiveRoles Server implementiert werden. Die Erstellung und Pflege komplexer, mehrere Schritte umfassende Prozesse auf diese Weise kann jedoch eine große Herausforderung darstellen. Arbeitsabläufe bieten einen anderen Ansatz. Sie ermöglichen IT-Administratoren die grafische Definition eines Verwaltungsprozesses. Dies kann schneller als die Erstellung des Prozesses durch Anwendung einzelner Richtlinien sein. Außerdem ist der Prozess so verständlicher, leichter zu erläutern und zu ändern.

Das Diagramm unten zeigt einen in der ActiveRoles Server-Konsole erstellten Arbeitsablauf. In diesem einfachen Beispiel überprüft der Arbeitsablauf bei einer Anforderung zum Hinzufügen eines Benutzers zu einer bestimmten Gruppe zunächst, ob die Gruppe über einen Besitzer verfügt. Wenn die Gruppe über keinen Besitzer verfügt, werden die angeforderten Änderungen verweigert, und der Arbeitsablauf ist abgeschlossen; andernfalls werden die Änderungen zur Genehmigung an den Besitzer der Gruppe weitergeleitet. Nach Erhalt der Genehmigung wendet ActiveRoles Server die Änderungen an und fügt den Benutzer zur Gruppe hinzu. Im Prozessdiagramm wird dieser Schritt als **Vorgangsausführung** bezeichnet. Wenn der Besitzer die Änderungen ablehnt, wird der Arbeitsablauf beim vorigen (Genehmigungs-) Schritt beendet, sodass die Änderungen nicht übernommen werden. Nach der Durchführung der Änderungen sendet der Arbeitsablauf eine E-Mail-Benachrichtigung an die Person, die die Änderungen angefordert hat, und wird dann beendet.



Im Beispiel oben verwaltet der Arbeitsablauf den Prozess des Hinzufügens eines Benutzers zu einer Gruppe gemäß den zum Zeitpunkt des Entwurfs des Arbeitsablaufs definierten Regeln. Die Regeln stellen die Arbeitsablaufdefinition dar und umfassen die Aktivitäten, die innerhalb des Prozesses durchgeführt werden, sowie die Beziehungen zwischen den Aktivitäten. Eine Aktivität in einer Prozessdefinition kann eine standardmäßig verfügbare, vordefinierte Funktion wie etwa eine Genehmigungsanforderung oder eine Benachrichtigung über Bedingungen, die das Eingreifen des Benutzers erfordern, oder eine benutzerdefinierte Funktion, die mit Hilfe von Skripttechnologien erstellt wurde, sein.

Ein Arbeitsablaufprozess wird gestartet, wenn die angeforderten Änderungen den in der Arbeitsablaufdefinition angegebenen Bedingungen entsprechen. Im Beispiel oben können die Bedingungen so eingerichtet werden, dass der Arbeitsablauf immer dann startet, wenn ein Benutzer von ActiveRoles Server Änderungen an der Mitgliedschaftsliste einer bestimmten Gruppe vorgenommen hat. Wenn die Bedingungen erfüllt sind, startet der Arbeitsablaufprozess, um die Änderungen durch die Arbeitsablaufdefinition zu leiten. Hierbei führt er automatisierte Schritte durch und fordert bei Bedarf eine Aktion von einer Person (wie etwa eine Genehmigung) an.

Übersicht über die Arbeitsablaufaktivitäten

Aktivitäten sind Arbeitseinheiten, von denen jede zur Erfüllung eines Arbeitsablaufprozesses beiträgt. ActiveRoles Server bietet eine Standardreihe von Aktivitäten, die eine vordefinierte Funktion für die Genehmigung, Benachrichtigung, den Kontrollfluss und Bedingungen ausführen. Damit eine Aktivität benutzerdefinierte Funktionen ausführt, können Skripts erstellt werden.

Aktivitäten sind die wesentlichen Bausteine für Arbeitsabläufe. Ein Arbeitsablauf ist im Grunde eine Reihe von Aktivitäten, die in einem Prozessdiagramm zusammengefasst sind. Wenn Sie einen Arbeitsablauf mit Hilfe des Workflow Designers errichten, ziehen Sie Aktivitäten aus dem Aktivitätsbereich auf der Prozessdiagramm und konfigurieren Sie sie dann dort. Die für alle Aktivitäten gemeinsamen konfigurierbaren Parameter lauten:

- **Name** Der Name wird verwendet, um die Aktivität im Arbeitsablaufdiagramm zu identifizieren.
- **Beschreibung** Dieser optionale Text ist nützlich für die Unterscheidung der Aktivitäten. Die Beschreibung wird angezeigt, wenn Sie mit der Maus auf die entsprechende Aktivität im Prozessdiagramm zeigen.

In den folgenden Abschnitten sind die Aktivitätstypen beschrieben, die in ActiveRoles Server enthalten sind. Die Abschnitte enthalten Informationen zu den für jeden Aktivitätstyp spezifischen, konfigurierbaren Parametern.

Skriptaktivität

Skriptaktivitäten werden üblicherweise verwendet, um automatisierte Schritte in einem Arbeitsablaufprozess durchzuführen. Eine Skriptaktivität wird durch ein in ActiveRoles Server erstelltes Skriptmodul definiert. Jedes Skriptmodul enthält einen Skriptcode, der bestimmte Funktionen implementiert. Neue Skriptmodule können frei hinzugefügt werden, und das in einem Skriptmodul enthaltene Skript kann bei Bedarf weiterentwickelt und überprüft werden. So können benutzerdefinierte Funktionen erstellt werden. Dies bietet die Möglichkeit, die von einem Arbeitsablauf durchgeführten Vorgänge zu erweitern.

Der einzige, für eine Skriptaktivität spezifische konfigurierbare Parameter ist der Verweis auf ein Skriptmodul. Wenn Sie eine Skriptaktivität zu einem Prozessdiagramm hinzufügen, werden Sie zur Auswahl des Skriptmoduls aufgefordert, das das von dieser Aktivität auszuführende Skript enthält.

Weitere Informationen und Anweisungen, die sich auf den Entwurf, die Implementierung und die Verwendung von Skripts, Skriptmodulen und Skriptaktivitäten beziehen, finden Sie in der Dokumentation zu ActiveRoles Server SDK.

Genehmigungsaktivität

Eine Genehmigungsaktivität, auch als „Genehmigungsregel" bezeichnet, stellt einen Entscheidungspunkt in einem Arbeitsablauf auf, der verwendet wird, um die Autorisierung von einer Person zu erhalten, bevor der Arbeitsablauf fortgesetzt werden kann. Die Arbeitsablauf-Startbedingungen geben an, welche Vorgänge den Arbeitsablauf starten. Die zum Arbeitsablauf hinzugefügten Genehmigungsregeln bestimmen, wer den Vorgang genehmigen soll, in welcher Reihenfolge die Genehmigungen erfolgen sollen und wer über Genehmigungsaufgaben oder Entscheidungen benachrichtigt werden soll.

ActiveRoles Server erstellt eine Genehmigungsaufgabe als Teil der Verarbeitung einer Genehmigungsregel und weist die Aufgabe dann genehmigenden Instanzen zu. Von der genehmigenden Instanz wird die Erfüllung der Aufgabe erwartet, d. h. sie muss die Entscheidung treffen, ob der Vorgang zulässig ist oder abgelehnt werden soll. Bis zum Abschluss der Aufgabe verbleibt der Vorgang im Status „Ausstehend".

Die für eine Genehmigungsaktivität spezifischen konfigurierbaren Parameter lauten:

- **Genehmigende Instanzen** Dies sind die Benutzer oder Benutzergruppen, die berechtigt sind, Genehmigungsaufgaben durchzuführen. Bei der Verarbeitung einer Genehmigungsregel erstellt ActiveRoles Server eine Genehmigungsaufgabe und weist sie dann den von der Regel definierten genehmigenden Instanzen zu. Der Status der Aufgabe bestimmt den Übergang des Arbeitsablaufs: die Aufgabe muss die Auflösung „Genehmigen" erhalten, damit der Vorgang der Genehmigungsregel entspricht. Wenn der Aufgabe die Auflösung „Zurückweisen" zugewiesen wird, wurde der Vorgang verweigert, und die Arbeitsablaufinstanz ist abgeschlossen.

  Genehmigende Instanzen können per Suche in den verfügbaren Benutzern und Gruppen ausgewählt werden. Es können auch bestimmte Funktionsinhaber als genehmigende Instanzen benannt werden. So kann zum Beispiel eine Genehmigungsregel so konfiguriert werden, dass die Genehmigung durch den Vorgesetzten der Person, die den Vorgang angefordert hat, oder vom Verwalter der Gruppe oder des Containers, die bzw. der von diesem Vorgang betroffen ist, erfolgen muss.

- **Benachrichtigung** Wird verwendet, um Empfänger als Abonnenten der Benachrichtigungen über Ereignisse im Zusammenhang mit der Genehmigung festzulegen, um Benachrichtigungs-E-Mails zu konfigurieren und um die E-Mail-Übertragung einzurichten. Genehmigungsregeln ermöglichen in Verbindung mit verschiedenen Ereignissen wie etwa der Erstellung von Genehmigungsaufgaben bei Vorgangsanforderungen die Benachrichtigung von Arbeitsablauf-Benutzern per E-Mail. So können genehmigende Instanzen über die Anforderungen, die durch sie genehmigt werden sollen, per E-Mail einschließlich Hypertext-Verknüpfungen zu dem mit der Genehmigung verbundenen Bereich im Web-Interface benachrichtigt werden. Eine Genehmigungsaktivität hat dieselben Benachrichtigungsparameter wie eine Benachrichtigungsaktivität.

Benachrichtigungsaktivität

Eine Benachrichtigungsaktivität in einem Arbeitsablauf wird verwendet, um eine E-Mail-Benachrichtigung über den Abschluss des Vorgangs, der den Arbeitsablauf gestartet hat, an die angegebenen Benutzer oder Gruppen zu senden. Wenn zum Beispiel ActiveRoles Server Self-Service den Benutzern ermöglicht, sich selbst zu einer Verteilerliste hinzuzufügen, können Sie eine Benachrichtigungsaktivität konfigurieren, die immer dann eine E-Mail an die Besitzer der Verteilerliste sendet, wenn Benutzer der Verteilerliste beitreten oder sie verlassen.

Die für eine Benachrichtigungsaktivität spezifischen, konfigurierbaren Parameter sind identisch mit den Benachrichtigungsparametern einer Genehmigungsaktivität. Sie sind nachfolgend aufgeführt:

- **Benachrichtigungsempfänger** Dies sind die Benutzer oder Gruppen, an die die Aktivität E-Mails sendet. Ein Empfänger kann jeder beliebige Postfach-fähige Benutzer oder jede E-Mail-fähige Gruppe sein. Es gibt auch eine Reihe von Optionen, die es Ihnen ermöglichen, Empfänger auf der Grundlage ihrer Funktion wie etwa ein Vorgangsanforderer, eine genehmigende Instanz, ein Vorgesetzter des Vorgangsanforderers oder ein Verwalter des von dem Vorgang betroffenen Objekts auszuwählen.
- **Benachrichtigungsübermittlung** Die Übermittlungsoptionen legen fest, ob Benachrichtigungen sofort oder auf einer geplanten Basis gesendet werden. Die Option der sofortigen Übermittlung führt dazu, dass die Aktivität bei jedem Eintritt des Ereignisses, bei dem eine Benachrichtigung erfolgen soll, eine separate Nachricht generiert. Die Option der geplanten Übermittlung kann für die Sammlung von Benachrichtigungen verwendet werden. Wenn sie sich für eine geplante Übermittlung entschließen, werden alle Benachrichtigungen über den Eintritt des Ereignisses innerhalb eines frei wählbaren Zeitraums gesammelt und als eine einzige Nachricht gesendet.
- **Benachrichtigungsmeldung** Benachrichtigungsmeldungen basieren auf einer Nachrichtenvorlage, die das Format und den Inhalt von E-Mail-Benachrichtigungen einschließlich des Nachrichtenbetreffs und Nachrichtentexts festlegt. Eine Vorlage ist ein Dokument im HTML-Format, das Sie anzeigen und bei Bedarf ändern können, um Benachrichtigungsmeldungen anzupassen. Der Vorlagentext kann dynamischen Inhalt umfassen, der bei Laufzeit durch Abfrage von Informationen aus der ausgeführten Instanz des Arbeitsablaufprozesses generiert wird.
- **Web-Interface-Adresse** Dieser Parameter wird verwendet, um die Adresse (URL) des ActiveRoles Server Web-Interface für die Erstellung von Hyperlinks in den Benachrichtigungsmeldungen anzugeben.
- **E-Mail-Server** Diese Einstellung gibt den Namen und andere Parameter des E-Mail-Servers an, der für die Übermittlung von Benachrichtigungsmeldungen verwendet wird.

Wenn-Dann-Sonst-Aktivität

Eine Wenn-Dann-Sonst-Aktivität wird verwendet, um einen von zwei oder mehr alternativen Zweigen abhängig von den für die Zweige definierten Bedingungen auszuführen. Sie enthält eine geordnete Reihe von Zweigen und führt den ersten Zweig aus, dessen Bedingung TRUE ist. Sie können so viele Zweige wie Sie möchten zu einer Wenn-Dann-Sonst-Aktivität hinzufügen, und Sie können auch so viele Aktivitäten wie Sie möchten zu jedem Zweig hinzufügen.

Für jeden Zweig einer Wenn-Dann-Sonst-Aktivität kann eine individuelle Bedingung festgelegt werden. Wenn eine Wenn-Dann-Sonst-Aktivität startet, prüft sie, ob die für ihren ersten (äußersten linken) Zweig festgelegte Bedingung wahr ist. Wenn die Bedingung erfüllt ist, werden die im Zweig enthaltenen Aktivitäten ausgeführt; andernfalls wird geprüft, ob die für den nächsten Zweig (von links nach rechts) festgelegte Bedingung wahr ist, etc.

Beachten Sie bei der Konfiguration von Wenn-Dann-Sonst-Zweigbedingungen folgende Hinweise:

- Nur der erste Zweig, dessen Bedingung TRUE ergibt, wird ausgeführt.
- Eine Wenn-Dann-Sonst-Aktivität kann beendet werden, ohne dass irgendeine ihrer Zweige ausgeführt wurde, wenn sich die für jeden Zweig festgelegte Bedingung als FALSE erweist.

Wenn keine Bedingung für einen Zweig definiert ist, so wird der Zweig so behandelt, as wenn eine permanent TRUE Bedingung vorliegt. Daher sollte der letzte (äußerst rechte) Zweig normalerweise über keine Bedingung verfügen, d. h. der Zweig sollte immer TRUE ergeben. Auf diese Weise fungiert der letzte Zweig als der „Sonst"-Zweig, der ausgeführt wird, wenn die Bedingungen für die anderen Zweige nicht erfüllt sind. Es ist ratsam, eine Bedingung für jeden Zweig in einer Wenn-Dann-Sonst-Aktivität mit Ausnahme des letzten Zweigs zu definieren, um zu gewährleisten, dass die Aktivität immer einen bestimmten Zweig ausführt.

Stoppen/Unterbrechen-Aktivität

Eine Stoppen/Unterbrechen-Aktivität wird verwendet, um sofort alle Aktivitäten einer laufenden Arbeitsablaufinstanz zu beenden. Sie können sie innerhalb eines Zweigs einer Wenn-Dann-Sonst-Aktivität verwenden, um den Arbeitsablauf zu beenden, wenn eine bestimmte Bedingung eintritt.

Als Beispiel dient eine Anforderung für die Bestätigung der angeforderten Datenänderungen, um bestimmte Vorgänge zu verweigern, weil die Anwendung solcher Vorgänge dazu führen würde, dass inakzeptable Daten in das Verzeichnis geschrieben werden. Um diese Anforderung zu erfüllen, können Sie einen Arbeitsablauf mit einem Wenn-Dann-Sonst-Zweig verwenden, der bei Erkennung inakzeptabler Daten im angeforderten Vorgang ausgeführt wird, und dann eine Stoppen/Unterbrechen-Aktivität zu diesem Zweig hinzufügen. Auf diese Weise sperrt Ihr Arbeitsablauf die unerwünschten Vorgänge und schützt so die Verzeichnisdaten.

Die Stoppen/Unterbrechen-Aktivität schreibt eine Nachricht ins Protokoll, wenn sie die Arbeitsablaufinstanz beendet. Sie können einen Nachrichtentext als einen Aktivitätsparameter festlegen, um den Grund für die Beendigung der Arbeitsablaufinstanz anzugeben. Die Aktivität umfasst diese Nachricht in dem Ereignis, das in das Ereignisprotokoll des ActiveRoles Server-Verwaltungsdienstes (das „EDM-Server"-Ereignisprotokoll) geschrieben wird.

Übersicht über die Arbeitsablaufverarbeitung

In ActiveRoles Server werden Verzeichnisobjekte wie etwa Benutzer, Gruppen oder Computer vom Verwaltungsdienst verwaltet. Diese Objekte können über Anforderungen, die an den Verwaltungsdienst gerichtet werden, erstellt, geändert oder gelöscht werden. Jede Anforderung startet einen Vorgang, um die angeforderten Änderungen an den Verzeichnisdaten vorzunehmen. So startet zum Beispiel eine Anforderung zur Erstellung eines Benutzers oder einer Gruppe den Erstellungsvorgang, wobei der Zielobjekttyp auf „Benutzer" bzw. „Gruppe" gesetzt ist; Eine Anforderung zum Hinzufügen von Benutzern zu einer Gruppe startet den Vorgang „Ändern" für diese Gruppe.

Wenn ein Vorgang gestartet wurde, startet der Verwaltungsdienst die Verarbeitung des Vorgangs. Jeder Vorgang wird durch ein einzelnes Objekt angegeben, das normalerweise als das Anforderungsobjekt bezeichnet wird und das alle für die Durchführung des Vorgangs erforderlichen Informationen enthält. Daher durchläuft das Anforderungsobjekt im Rahmen der Vorgangsverarbeitung eine Reihe von Phasen innerhalb des Verwaltungsdienstes.

Das Vorgangsverarbeitungsmodell in ActiveRoles Server besteht aus vier Hauptphasen: Zugriffskontrolle, Vorausführung, Ausführung und Nachausführung. Das Anforderungsobjekt durchläuft diese Phasen in der folgenden Reihenfolge:

- **Zugriffskontrolle** In dieser Phase überprüft der Verwaltungsdienst, ob der Benutzer oder das System, der bzw. das die Anforderung gestellt hat, über ausreichende Rechte zur Durchführung der angeforderten Änderungen verfügt. Bei unzureichenden Rechten wird der Vorgang verweigert.

- **Vorausführung** Während dieser Phase führt der Verwaltungsdienst zunächst die Vorausführungs-Arbeitsablaufaktivitäten aus. Dies sind die Aktivitäten, die sich im oberen Teil des Arbeitsablaufprozessdiagramms über der Zeile **Vorgangsausführung** befinden. Ein typisches Beispiel sind Genehmigungsaktivitäten: An diesem Punkt können die genehmigenden Instanzen den Vorgang zulassen oder ablehnen.

  Wenn die Vorausführungsaktivitäten abgeschlossen wurden, ohne dass der Vorgang zurückgewiesen wurde, führt der Verwaltungsdienst die Vorausführungsrichtlinien aus. Typische Beispiele für solche Richtlinien umfassen die Erstellung von Eigenschaften und Bestätigungsregeln sowie die Funktionen, die so genannte „Vorereignis-Handler" in Skriptrichtlinien implementieren.

- **Ausführung** In dieser Phase führt der Verwaltungsdienst den Vorgang aus und nimmt die angeforderten Änderungen an den Verzeichnisdaten vor. Wenn beispielsweise die Erstellung eines Benutzer angefordert ist, wird der Benutzer in dieser Phase erstellt.
- **Nachausführung** Während dieser Phase führt der Verwaltungsdienst zunächst die Nachausführungsrichtlinien aus. So erfolgt zum Beispiel bei der Erstellung eines Benutzers in dieser Phase die Bereitstellung eines Stammordners oder von Gruppenmitgliedschaften für diesen Benutzer. Die Funktionen, die „Nachereignis-Handlers" in Skriptrichtlinien implementieren, werden ebenfalls in diesem Schritt ausgeführt.

  Schließlich führt der Verwaltungsdienst nach beendeter Ausführung der Nachausführungsrichtlinien die Nachausführungs-Arbeitsablaufaktivitäten aus. Dies sind die Aktivitäten, die sich im unteren Teil des Arbeitsablaufprozessdiagramms unter der Zeile **Vorgangsausführung** befinden. Ein typisches Beispiel sind Benachrichtigungsaktivitäten, die E-Mail versenden, die über den Abschluss des Vorgangs informieren.

Der Verwaltungsdienst führt die Arbeitsablaufaktivitäten nacheinander in der im Arbeitsablaufprozessdiagramm gezeigten sequenziellen Reihenfolge aus, bis die letzte Aktivität beendet ist. Wenn-Dann-Sonst-Aktivitäten können verwendet werden, um eine bedingte Verzweigung in Arbeitsabläufen zu erreichen. Diese Verzweigungen ermöglichen die Änderung der Reihenfolge von Aktivitäten abhängig von den an der Anforderung involvierten Daten.

Zu Beginn der Vorausführungsphase legt der Verwaltungsdienst die zu startenden Arbeitsabläufe fest. Die Anforderung wird mit allen vorhandenen Arbeitsablaufdefinitionen verglichen. Damit ein Arbeitsablauf startet, muss der angeforderte Vorgang die für diesen Arbeitsablauf definierten Startbedingungen erfüllen. Wenn die Startbedingungen erfüllt sind wird der Arbeitsablauf an die Anforderung angepasst.

Für einen Arbeitsablauf, der an die Anforderung angepasst wird, führt der Verwaltungsdienst die Aktivitäten aus, die in diesem Arbeitsablauf während der entsprechenden Phasen der Vorgangsverarbeitung gefunden wurden. Nur ein Arbeitsablauf oder mehrere Arbeitsabläufe können an eine einzelne Anforderung angepasst werden. Bei mehreren Arbeitsabläufen startet der Verwaltungsdienst jeden dieser Abläufe einzeln nacheinander und führt zunächst alle in diesen Arbeitsabläufen enthaltenen Vorausführungsaktivitäten aus. Dann führt der Verwaltungsdienst während der Nachausführungsphase alle in diesen Arbeitsabläufen enthaltenen Nachausführungsaktivitäten aus.

Startbedingungen

Um einen Arbeitsablauf in ActiveRoles Server bereitzustellen, erstellen Sie eine Arbeitsablaufdefinition, konfigurieren dann die Startbedingungen für diesen Arbeitsablauf, fügen Arbeitsablaufaktivitäten hinzu und konfigurieren diese. Bei der Konfiguration von Arbeitsablauf-Startbedingungen geben Sie Folgendes an:

- Vorgangstyp wie etwa Erstellen, Umbenennen, Ändern oder Löschen; der Arbeitsablauf wird nur dann an die Anforderung angepasst, wenn ein Vorgang dieses Typs angefordert ist.
- Objekttyp wie etwa Benutzer, Gruppe oder Computer; der Arbeitsablauf wird nur dann an die Anforderung angepasst, wenn der Vorgang Änderungen an einem Objekt dieses Typs anfordert.
- Für den Vorgangstyp „Ändern" eine Liste der Objekteigenschaften; der Arbeitsablauf wird nur dann an die Anforderung angepasst, wenn der Vorgang Änderungen an irgendeiner dieser Eigenschaften eines Objekts anfordert.
- Identität eines Vorgangsanforderers (Initiator) wie etwa ein Benutzer, eine Gruppe oder ein Dienst; der Arbeitsablauf wird nur dann an die Anforderung angepasst, wenn der Vorgang im Namen dieser Identität angefordert wird.
- Container wie etwa eine Organisationseinheit oder eine verwaltete Einheit; der Arbeitsablauf wird nur dann an die Anforderung angepasst, wenn der Vorgang Änderungen an bzw. die Erstellung von einem Objekt in diesem Container anfordert.
- Optional ein Filter, der alle zusätzlichen Bedingungen für die an einem Vorgang beteiligten Einheiten definiert; der Arbeitsablauf wird nur dann an die Anforderung angepasst, wenn der Vorgang diesen Bedingungen entspricht. Wenn kein Filter festgelegt ist, dann sind keine zusätzlichen Bedingungen gültig.

Bei einer Anforderung für einen beliebigen Vorgang, die alle für einen Arbeitsablauf angegebenen Startbedingungen erfüllt, passt der Verwaltungsdienst den Arbeitsablauf an die Anforderung an und führt die im Arbeitsablauf gefundenen Aktivitäten aus.

Konfigurieren eines Arbeitsablaufs

Arbeitsabläufe stellen eine leistungsfähige und bequeme Methode zum Hinzufügen einer neuen Logik zur Verzeichnisdatenverwaltungs- und -bereitstellungsprozessen in ActiveRoles Server dar. Um einen Arbeitsablauf zu konfigurieren, erstellen Sie eine Arbeitsablaufdefinition und verwenden dann den Workflow Designer, um Arbeitsablaufaktivitäten hinzuzufügen und zu konfigurieren.

Dieser Abschnitt deckt die folgenden Aufgaben ab:

- Erstellen einer Arbeitsablaufdefinition
- Konfigurieren der Startbedingungen für einen Arbeitsablauf
- Hinzufügen von Aktivitäten zu einem Arbeitsablauf
- Konfigurieren einer Skriptaktivität
- Konfigurieren einer Genehmigungsaktivität
- Konfigurieren einer Benachrichtigungsaktivität
- Konfigurieren einer Wenn-Dann-Sonst-Aktivität
- Konfigurieren einer Stoppen/Unterbrechen-Aktivität
- Aktivieren oder Deaktivieren eines Arbeitsablaufs

Erstellen einer Arbeitsablaufdefinition

Die ActiveRoles Server-Konsole enthält den Workflow Designer zum Erstellen und Konfigurieren von Arbeitsabläufen. Zunächst erstellen Sie eine Arbeitsablaufdefinition. Dann verwenden Sie den Workflow Designer, um einen Arbeitsablauf zu erstellen und die Arbeitsablauf-Konfigurationsdaten in der Arbeitsablaufdefinition zu speichern.

Gehen Sie folgendermaßen vor, um eine Arbeitsablaufdefinition zu erstellen:

1. Erweitern Sie in der ActiveRoles Server-Konsolenstruktur **Configuration | Policies**, klicken Sie dann mit der rechten Maustaste auf **Workflow** und wählen Sie **Neu | Arbeitsablaufrichtlinie**.
2. Geben Sie im Assistenten zur Erstellung neuer Objekte einen Name und optional eine Beschreibung für den neuen Arbeitsablauf ein.
3. Folgen Sie den Anweisungen des Assistenten, um die Erstellung der Arbeitsablaufdefinition fertigzustellen.

Wenn Sie eine Arbeitsablaufdefinition erstellt haben, können Sie sie im Workflow Designer öffnen, um Arbeitsablaufaktivitäten wie etwa Genehmigungsregeln hinzuzufügen und Arbeitsablauf-Startbedingungen anzugeben.

Konfigurieren der Startbedingungen für einen Arbeitsablauf

Die Arbeitsablauf-Startbedingungen legen fest, welche Vorgänge zum Start des Arbeitsablaufs führen. Ein Genehmigungs-Arbeitsablauf kann zum Beispiel so konfiguriert sein, dass jede Anforderung zur Erstellung eines Benutzers in einem bestimmten Container den Arbeitsablauf startet und somit die Genehmigung für die Anforderung erfordert. Sie können die Startbedingungen für einen Arbeitsablauf festlegen, indem Sie seine Definition im Workflow Designer bearbeiten.

Gehen Sie folgendermaßen vor, um die Startbedingungen für einen Arbeitsablauf anzuzeigen oder zu ändern:

1. Erweitern Sie in der ActiveRoles Server-Konsolenstruktur **Configuration | Policies | Workflow** und wählen Sie dann den Arbeitsablauf, den Sie konfigurieren möchten.

   Hierdurch wird das Workflow Designer-Fenster im Bereich „Details" geöffnet, das die Arbeitsablaufdefinition als ein Prozessdiagramm darstellt.

2. Klicken Sie im Bereich „Details" auf die Verknüpfung über dem Prozessdiagramm.

   *Hierdurch wird das Dialogfeld **Arbeitsablauf-Startbedingungen** angezeigt, in dem Sie Vorgangsbedingungen, Initiatorbedingungen und Filterbedingungen anzeigen oder ändern können.*

Vorgangsbedingungen

Die Vorgangsbedingungen legen Folgendes fest:

- Einen Objekttyp wie etwa Benutzer, Gruppe oder Computer; der Arbeitsablauf startet nur dann, wenn ein Vorgang Änderungen an einem Objekt dieses Typs anfordert.
- Einen Vorgangstyp wie etwa Erstellen, Umbenennen, Ändern oder Löschen; der Arbeitsablauf startet nur dann, wenn ein Vorgang dieses Typs angefordert wird.
- Für den Vorgangstyp „Ändern" eine Liste der Objekteigenschaften; der Arbeitsablauf startet nur dann, wenn ein Vorgang Änderungen an irgendeiner dieser Eigenschaften eines Objekts anfordert.

Gehen Sie folgendermaßen vor, um die Vorgangsbedingungen anzuzeigen oder zu ändern:

1. Klicken Sie im Dialogfeld **Arbeitsablauf-Startbedingungen** auf **Vorgang auswählen**.
   Hierdurch wird eine Seite geöffnet, auf der Sie den Objekttyp und die Vorgangstypeinstellungen anzeigen oder ändern können.
2. Um die Objekttypeinstellungen zu ändern, wählen Sie einen Objekttyp aus dem Dropdown-Listenfeld aus.
   Um einen Objekttyp auszuwählen, der nicht im Dropdown-Listenfeld enthalten ist, klicken Sie auf die Schaltfläche neben dem Dropdown-Listenfeld.
3. Um die Vorgangstypeinstellung zu ändern, klicken Sie auf die entsprechende Option.
4. Wenn der Vorgangstyp „Ändern" (die Option **Eigenschaften bearbeiten**) ausgewählt ist, klicken Sie auf **Weiter**, um die Auswahl der Eigenschaften anzuzeigen oder zu ändern.
5. Klicken Sie auf **Fertig stellen**.

Initiatorbedingungen

Die Initiatorbedingungen legen Folgendes fest:

- Identität eines Vorgangsanforderers (Initiator) wie etwa ein Benutzer, eine Gruppe oder eine Anwendung; der Arbeitsablauf startet nur dann, wenn ein Vorgang im Namen dieser Identität angefordert wird.
- Container wie etwa eine Organisationseinheit oder eine verwaltete Einheit; der Arbeitsablauf startet nur dann, wenn ein Vorgang Änderungen an bzw. die Erstellung von einem Objekt in diesem Container anfordert.

Gehen Sie folgendermaßen vor, um die Initiatorbedingungen anzuzeigen oder zu ändern:

1. Beobachten Sie im Dialogfeld **Arbeitsablauf-Startbedingungen** die Liste im Bereich **Initiator-Bedingungen**.
   Jeder Eintrag in der Liste steht für eine einzelne Initiatorbedingung, wobei das erste Feld den Vorgangsanforderer und das zweite Feld den Container angibt. Wenn keine Liste vorhanden ist, sind keine Initiatorbedingungen definiert.
2. Gehen Sie folgendermaßen vor, um eine Initiatorbedingung zu definieren:
   a) Klicken Sie auf **Hinzufügen** im Bereich **Initiator-Bedingungen**.
   b) Füllen Sie die Liste der Vorgangsanforderer aus.
   c) Wählen Sie den Container.
3. Um eine Initiatorbedingung zu löschen, wählen Sie den entsprechenden Eintrag aus der Liste **Initiatorbedingungen** aus, und klicken Sie dann auf **Entfernen**.

Wenn mehrere Initiatorbedingungen definiert sind, startet der Arbeitsablauf, wenn eine dieser Bedingungen erfüllt ist.

Wenn mehrere Vorgangsanforderer innerhalb einer einzigen Initiatorbedingung definiert sind, wird die Bedingung als erfüllt betrachtet, wenn der Vorgang von einer dieser Identitäten angefordert wird.

Filterbedingungen

Ein Filter kann verwendet werden, um jegliche zusätzlichen Bedingungen für die an einem Vorgang beteiligten Objekte zu definieren. Der Arbeitsablauf startet nur dann, wenn der Vorgang diesen Bedingungen entspricht. Wenn kein Filter festgelegt ist, dann sind keine zusätzlichen Bedingungen gültig.

Filterbedingungen können auf den Eigenschaften der Objekte beruhen, die an der Vorgangsanforderung beteiligt sind. Alternativ kann auch ein Skript verwendet werden, um komplexe Filterbedingungen zu implementieren. Filterbedingungen können auf den Eigenschaften der folgenden Elemente basieren:

- **Initiator** Der Arbeitsablauf startet nur, wenn bestimmte Eigenschaften des Vorgangsanforderers bestimmte Bedingungen erfüllen. Diese Option kann zum Beispiel verwendet werden, um eine Genehmigung für Vorgänge zu fordern, die von Personen mit einer bestimmten Funktion oder aus einer bestimmten Abteilung initiiert werden.
- **Zielobjekt** Der Arbeitsablauf startet nur, wenn bestimmte Eigenschaften des Zielobjekts des Vorgangs bestimmte Bedingungen erfüllen. Diese Option kann zum Beispiel verwendet werden, um eine Genehmigung für Änderungen an Gruppen mit bestimmten Namen zu fordern.
- **Änderungsanforderung** Der Arbeitsablauf startet nur, wenn die angeforderten Änderungen bestimmte Bedingungen erfüllen. Diese Option kann zum Beispiel verwendet werden, um eine Genehmigung für Änderungen zu fordern, die spezifisch für bestimmte Eigenschaften wie etwa das Benutzer-Logon sind oder in Verbindung mit E-Mail-relevanten Eigenschaften stehen.
- **Quellcontainer** Die Verschiebung eines Objekts startet den Arbeitsablauf nur, wenn der Container, in dem sich das Objekt befindet, bestimmte Bedingungen erfüllt. Diese Option kann zum Beispiel verwendet werden, um eine Genehmigung für Vorgänge zu fordern, bei denen Objekte aus einem Container mit einer bestimmten Beschreibung verschoben werden.
- **Zielcontainer** Die Verschiebung eines Objekts startet den Arbeitsablauf nur, wenn der Container, in den das Objekt verschoben werden soll, bestimmte Bedingungen erfüllt. Diese Option kann zum Beispiel verwendet werden, um eine Genehmigung für Vorgänge zu fordern, bei denen Objekte in einen Container mit einer bestimmten Beschreibung verschoben werden.

Gehen Sie folgendermaßen vor, um Filterbedingungen auf der Grundlage von Objekteigenschaften zu konfigurieren:

1. Klicken Sie im Dialogfeld **Arbeitsablauf-Startbedingungen** auf **Filterung konfigurieren**.
2. Klicken Sie auf der Seite **Filterung konfigurieren** auf **Hinzufügen** und klicken Sie dann auf die entsprechende Option (die Liste der verfügbaren Optionen ist von den Vorgangstyp-einstellungen abhängig):
   - Klicken Sie auf **Initiator**, um eine Bedingung auf der Grundlage der Eigenschaften des Vorgangsanforderers hinzuzufügen.
   - Klicken Sie auf **Vorgangsziel**, um eine Bedingung auf der Grundlage der Eigenschaften des Zielobjekts des Vorgangs hinzuzufügen.
   - Klicken Sie auf **Neues Objekt** oder **Geänderte Eigenschaft**, um eine Bedingung auf der Grundlage von Eigenschaften hinzuzufügen, die der Vorgang festlegen oder ändern soll.
   - Klicken Sie auf **Quellcontainer**, um eine Bedingung auf der Grundlage von Eigenschaften des Containers hinzuzufügen, aus dem der Vorgang ein Objekt verschieben wird.
   - Klicken Sie auf **Zielcontainer**, um eine Bedingung auf der Grundlage von Eigenschaften des Containers hinzuzufügen, in den der Vorgang ein Objekt verschieben wird.

3. Verwenden Sie das Dialogfeld **Bedingung konfigurieren**, um die Bedingung einzurichten:
   a) Klicken Sie auf die Schaltfläche **Eigenschaft** und wählen Sie die Eigenschaft aus, die die Bedingung prüfen soll.
   b) Klicken Sie im Bereich **Operator** auf die gewünschte Bedingungsvariable und geben Sie dann im Feld **Wert** einen Eigenschaftswert ein – die Bedingung wird als erfüllt betrachtet, wenn die ausgewählte Eigenschaft mit dem von Ihnen angegebenen Operator/Wert-Paar übereinstimmt.
   c) Klicken Sie auf **OK**.
4. Um weitere Bedingungen hinzuzufügen, wiederholen Sie die Schritte 2-3.
   Sie können mehrere Bedingungen hinzufügen. In diesem Fall werden die Bedingungen per UND zusammengeführt, was bedeutet, dass der Arbeitsablauf nur startet, wenn alle Bedingungen erfüllt sind. Sie können den Operator UND in ODER ändern, indem Sie auf den Eintrag UND in der Liste der Bedingungen doppelklicken.
5. Wenn Sie die Konfiguration der Bedingungen abgeschlossen haben, klicken Sie auf der Seite **Filterung konfigurieren** auf **Fertig stellen**.

Skriptbasierte Bedingungen

Um eine skriptbasierte Bedingung zu implementieren, müssen Sie ein Skriptmodul erstellen und anwenden, das eine Funktion enthält, die den angeforderten Vorgang analysiert, um zu ermitteln, ob der Arbeitsablauf gestartet werden soll oder nicht. Die Funktion kann den ADSI-Provider von ActiveRoles Server verwenden, um auf die Eigenschaften der am Vorgang beteiligten Objekte zuzugreifen, um die Eigenschaften zu analysieren und um dann abhängig von den Ergebnissen der Analyse den Wert TRUE oder FALSE auszugeben. Der Arbeitsablauf startet, wenn die Funktion TRUE ausgibt.

Gehen Sie folgendermaßen vor, um die skriptbasierte Bedingung anzuwenden:

1. Klicken Sie auf der Seite **Filterung konfigurieren** auf **Hinzufügen** und klicken Sie dann auf **Skript**.
2. Verwenden Sie das Dialogfeld **Skriptbedingung konfigurieren**, um das Skriptmodul auszuwählen und die Funktion anzugeben, die die anzuwendende Bedingung definiert.

Weitere Informationen und Anweisungen finden Sie im Abschnitt „Entwickeln von skriptbedingten Funktionen" in der ActiveRoles Server SDK and Resource Kit-Dokumentation.

Hinzufügen von Aktivitäten zu einem Arbeitsablauf

Die ActiveRoles Server-Konsole enthält den Workflow Designer zum Erstellen und Konfigurieren von Arbeitsabläufen. Zunächst erstellen Sie eine Arbeitsablaufdefinition. Verwenden Sie dann den Workflow Designer, um den Arbeitsablauf durch Hinzufügen und Konfigurieren von Arbeitsablaufaktivitäten zu erstellen.

Gehen Sie folgendermaßen vor, um eine Aktivität zu einem Arbeitsablauf hinzuzufügen:

1. Erweitern Sie in der ActiveRoles Server-Konsolenstruktur **Configuration | Policies | Workflow** und wählen Sie dann den Arbeitsablauf, zu dem Sie eine Aktivität hinzufügen möchten.
   Hierdurch wird das Workflow Designer-Fenster im Bereich „Details" geöffnet, das die Arbeitsablaufdefinition als ein Prozessdiagramm darstellt.
2. Ziehen Sie im Bereich „Details" die Aktivität vom linken Bereich auf das Prozessdiagramm.
3. Klicken Sie mit der rechten Maustaste auf den Namen der Aktivität auf dem Prozessdiagramm und klicken Sie dann auf **Eigenschaften**.
4. Verwenden Sie das Dialogfeld **Eigenschaften**, um die Aktivität zu konfigurieren. Die Anweisungen sind weiter unten in diesem Kapitel aufgeführt.

Wenn Sie eine Aktivität zum oberen Teil des Diagramms hinzufügen (über der Zeile **Vorgangs-ausführung**), dann wird die Aktivität in der Vorausführungsphase der Vorgangsverarbeitung ausgeführt (siehe „Übersicht über die Arbeitsablaufverarbeitung" weiter oben in diesem Kapitel). Bestimmte Aktivitäten wie etwa eine Benachrichtigungsaktivität, die für eine Aufführung in der Nachausführungsphase konzipiert sind, können nicht zum oberen Teil des Diagramms hinzugefügt werden.

Wenn Sie eine Aktivität zum unteren Teil des Diagramms hinzufügen (unter der Zeile **Vorgangs-ausführung**), dann wird die Aktivität in der Nachausführungsphase der Vorgangsverarbeitung ausgeführt. Bestimmte Aktivitäten wie etwa eine Genehmigungsaktivität, die für eine Aufführung in der Vorausführungsphase konzipiert sind, können nicht zum unteren Teil des Diagramms hinzugefügt werden.

Im Dialogfeld **Eigenschaften** können Sie den Namen und die Beschreibung der Aktivität ändern. Diese Einstellungen gelten für alle Aktivitäten. Der Name gibt die Aktivität auf dem Prozessdiagramm an. Die Beschreibung wird als ein QuickInfo angezeigt, wenn Sie auf die Aktivität zeigen.

Um eine Aktivität aus dem Prozessdiagramm zu entfernen, klicken Sie mit der rechten Maustaste auf den Namen der Aktivität und klicken Sie dann auf **Löschen**.

Konfigurieren einer Skriptaktivität

Bei der Konfiguration einer Skriptaktivität wählen Sie das Skriptmodul aus, das das Skript enthält, das von der Aktivität ausgeführt werden soll. Informationen und Anweisungen bezüglich der Erstellung eines Skripts für eine Skriptaktivität finden Sie in der Dokumentation zum ActiveRoles Server Software Development Kit (SDK).

Gehen Sie folgendermaßen vor, um eine Skriptaktivität zu konfigurieren:

1. Erweitern Sie in der ActiveRoles Server-Konsolenstruktur **Configuration | Policies | Workflow** und wählen Sie dann den Arbeitsablauf, der die Skriptaktivität enthält, die Sie konfigurieren möchten.

   Hierdurch wird das Workflow Designer-Fenster im Bereich „Details" geöffnet, das die Arbeitsablaufdefinition als ein Prozessdiagramm darstellt.

2. Klicken Sie im Prozessdiagramm mit der rechten Maustaste auf den Namen der Aktivität und klicken Sie dann auf **Eigenschaften**.
3. Führen Sie eine der folgenden Aktionen durch:
   - Wenn für die Aktivität kein Skriptmodul ausgewählt ist (beispielsweise wenn die Aktivität gerade zum Prozessdiagramm hinzugefügt wurde), wählen Sie das Skriptmodul aus, das das Skript enthält, das die Aktivität ausführen soll.
   - Wenn für die Aktivität bereits ein Skriptmodul ausgewählt ist und Sie ein anderes Skriptmodul verwenden möchten, klicken Sie auf die Schaltfläche **Durchsuchen**, um das gewünschte Skriptmodul auszuwählen.

Konfigurieren einer Genehmigungsaktivität

Bei der Konfiguration einer Genehmigungsaktivität innerhalb eines Arbeitsablaufs geben Sie Folgendes an:

- Genehmigende Instanzen wie etwa Benutzer oder Gruppen; diese Einstellung gibt die Personen an, die autorisiert sind, Vorgänge zuzulassen oder zu verweigern, die den Arbeitsablauf starten.
- Benachrichtigungseinstellungen wie etwa Arbeitsablaufereignisse, bei deren Eintreten eine Benachrichtigung erfolgen soll, Benachrichtigungsempfänger, Übermittlungsoptionen und die Benachrichtigungsmeldungsvorlage.

Dieser Abschnitt enthält für die Konfiguration von genehmigenden Instanzen spezifische Anweisungen: Anweisungen bezüglich der Konfiguration von Benachrichtigungseinstellungen finden Sie unter „Konfigurieren einer Benachrichtigungsaktivität" weiter unten in diesem Kapitel.

Gehen Sie folgendermaßen vor, um genehmigende Instanzen anzugeben:

1. Erweitern Sie in der ActiveRoles Server-Konsolenstruktur **Configuration | Policies | Workflow** und wählen Sie dann den Arbeitsablauf, der die Genehmigungsaktivität enthält, die Sie konfigurieren möchten.

   Hierdurch wird das Workflow Designer-Fenster im Bereich „Details" geöffnet, das die Arbeitsablaufdefinition als ein Prozessdiagramm darstellt.

2. Klicken Sie im Prozessdiagramm mit der rechten Maustaste auf den Namen der Genehmigungsaktivität und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie im Dialogfeld **Eigenschaften** auf die Registerkarte **Genehmigende Instanzen** und klicken Sie dann auf die Schaltfläche **Genehmigende Instanzen bestimmen**.
4. Aktivieren Sie auf der Seite **Genehmigende Instanzen bestimmen** die entsprechenden Kontrollkästchen, um genehmigende Instanzen festzulegen.
5. Wenn Sie das Kontrollkästchen **Diese Benutzer und Gruppen** aktiviert haben, verwenden Sie die Schaltflächen **Hinzufügen** und **Entfernen**, um die Liste der genehmigenden Instanzen zu konfigurieren.

Die Auswahl der genehmigenden Instanzen kann auf der Eigenschaft „Verwalter" oder „Verwaltet von" basieren:

- Durch Aktivierung des Kontrollkästchens **Verwalter der Person, die den Vorgang angefordert hat** konfigurieren Sie die Genehmigungsaktivität, sodass die von einem bestimmten Benutzer angeforderten Vorgänge die Genehmigung vom Verwalter dieses Benutzers erfordern. Bei Auswahl dieser Option sendet der vom Benutzer initiierte Vorgang die Genehmigungsaufgabe an die als Verwalter des Benutzers im Verzeichnis angegebene Person.
- Durch Aktivierung des Kontrollkästchens **Verwalter des Zielobjekts des Vorgangs** oder **Verwalter der Organisationseinheit, in der sich das Zielobjekt des Vorgangs befindet** konfigurieren Sie die Genehmigungsaktivität, sodass die Änderungen an einem bestimmten Objekt die Genehmigung von dem Verwalter des Objekts oder vom Verwalter der Organisationseinheit, die das Objekt enthält, erfordert. Bei Auswahl dieser Optionen sendet der Vorgang, der Änderungen an einem bestimmten Objekt fordert, die Genehmigungsaufgabe an die als Verwalter des Objekts oder der Organisationseinheit in dem Verzeichnis angegebene Person.

Die Auswahl von genehmigenden Instanzen kann auf einer Skriptfunktion basieren, die die genehmigende Instanz auswählt, wenn die Genehmigungsaktivität ausgeführt wird. Die Funktion kann den ADSI-Provider von ActiveRoles Server verwenden, um auf die Eigenschaften der am Vorgang beteiligten Objekte zuzugreifen, um die Eigenschaften zu analysieren und um eine Kennung des Benutzers oder der Gruppe auszugeben, die als genehmigende Instanz ausgewählt werden soll. Weitere Informationen und Anweisungen finden Sie im Abschnitt „Entwickeln von Funktion für die Festlegung von genehmigenden Instanzen" in der ActiveRoles Server SDK and Resource Kit-Dokumentation.

Konfigurieren einer Benachrichtigungsaktivität

Bei der Konfiguration einer Benachrichtigungsaktivität können Sie Benachrichtigungseinstellungen wie etwa Arbeitsablaufereignisse, bei deren Eintreten eine Benachrichtigung erfolgen soll, Benachrichtigungsempfänger, Übermittlungsoptionen und die Benachrichtigungsmeldungsvorlage festlegen. Dieselben Einstellungen gelten für den Abschnitt „Benachrichtigung" einer Genehmigungsaktivität.

Gehen Sie folgendermaßen vor, um die Benachrichtigungseinstellungen anzuzeigen oder zu ändern:

1. Erweitern Sie in der ActiveRoles Server-Konsolenstruktur **Configuration | Policies | Workflow** und wählen Sie dann den Arbeitsablauf, der die Genehmigungsaktivität oder Benachrichtigungsaktivität enthält, die Sie konfigurieren möchten.

   Hierdurch wird das Workflow Designer-Fenster im Bereich „Details" geöffnet, das die Arbeitsablaufdefinition als ein Prozessdiagramm darstellt.

2. Klicken Sie im Prozessdiagramm mit der rechten Maustaste auf den Namen der Aktivität und klicken Sie dann auf **Eigenschaften**.
3. Wenn Sie eine Genehmigungsaktivität ausgewählt haben, klicken Sie auf die Registerkarte **Benachrichtigung**.

Die Seite zur Konfiguration von Benachrichtigungen umfasst drei Bereiche:

- **Ereignisse, Empfänger und Nachrichten** In diesem Bereich können Sie Benachrichtigungen, von denen jede ein Ereignis angibt, bei dessen Eintritt eine Benachrichtigung erfolgen soll, sowie die Empfänger der Benachrichtigungsmeldung, die Nachrichtenübermittlungsoptionen und die Nachrichtenvorlage hinzufügen, anzeigen, ändern oder entfernen.
- **ActiveRoles Server Web-Interface** Dieser Bereich wird verwendet, um die Adresse (URL) des ActiveRoles Server Web-Interface für die Erstellung von Hyperlinks in den Benachrichtigungsmeldungen anzugeben.
- **E-Mail-Servereinstellungen** In diesem Bereich können Sie den Namen und andere Parameter des E-Mail-Servers, der für die Übermittlung von Benachrichtigungsmeldungen verwendet wird, anzeigen oder ändern.

Ereignisse, Empfänger und Nachrichten

Gehen Sie folgendermaßen vor, um eine Benachrichtigung hinzuzufügen:

1. Klicken Sie im Bereich **Ereignisse, Empfänger und Nachrichten** auf **Hinzufügen**.
2. Klicken Sie im Dialogfeld **Benachrichtigungseinstellungen** unter **Ereignis auswählen** auf das Ereignis, bei dessen Eintritt eine Benachrichtigung erfolgen soll.
3. Aktivieren Sie unter **Benachrichtigungsempfänger** die entsprechenden Kontrollkästchen, um die Benachrichtigungsempfänger anzugeben.

4. Wählen Sie unter **Benachrichtigungszustellung** die gewünschten Übermittlungsoptionen aus:
   - Wählen Sie **Sofort**, wenn die Benachrichtigungsmeldung bei jedem Eintreten des Ereignisses sofort gesendet werden soll.
   - Wählen Sie **Geplant**, wenn die Benachrichtigungsmeldungen innerhalb eines bestimmten Zeitraums gruppiert und als eine einzige Nachricht gesendet werden soll; klicken Sie dann auf **Konfigurieren**, um den Zeitraum anzugeben.
5. Klicken Sie unter **Benachrichtigungsmeldung** auf **Ändern**, um die Nachrichtenvorlage einschließlich des Betreffs und des Texts der Benachrichtigungsmeldung anzuzeigen oder zu ändern.
6. Klicken Sie auf **OK**, um das Dialogfeld **Benachrichtigungseinstellungen** zu schließen.

Benachrichtigungen können so konfiguriert werden, dass Benachrichtigungsmeldungen zusammengefasst und auf geplanter Basis versendet werden. Wenn Sie die Option **Geplant** unter **Benachrichtigungszustellung** auswählen, werden die Nachrichten innerhalb eines bestimmten, geplanten Zeitraums in einem temporären Speicher gesammelt, anstatt bei Eintritt des Ereignisses sofort gesendet zu werden. Nach Ablauf der festgelegten Dauer werden alle zusammengefassten Nachrichten als eine einzige Nachricht gesendet. Diese Option verhindert, dass das Arbeitsablaufsystem überflüssige Nachrichten sendet, und gewährleistet gleichzeitig, dass die Benachrichtigungsempfänger eine übersichtliche Zusammenfassung aller Ereignisse erhalten, die innerhalb des festgelegten Zeitraums aufgetreten sind. Klicken Sie auf die Schaltfläche **Konfigurieren** neben der Option **Geplant**, um den Versand der Benachrichtigungsmeldungen zu planen.

Durch Anklicken der Schaltfläche **Ändern** unter **Benachrichtigungsmeldung** wird ein Fenster geöffnet, in dem Sie die E-Mail-Benachrichtigungsvorlagen anzeigen und ändern können. Für jedes Ereignis (wie etwa „Aufgabe erstellt" oder „Vorgang durchgeführt") legt die Benachrichtigungskonfiguration eine Standardvorlage fest, auf deren Grundlage ActiveRoles Server E-Mail-Benachrichtigungen generiert. Jede Vorlage umfasst ein XHTML-Markup sowie den Text und Token, die Informationen über das Ereignis enthalten.

Damit die Benachrichtigungsmeldungen für die Empfänger aussagekräftiger sind, bieten Benachrichtigungsvorlagen die Möglichkeit, Token in die Nachrichten aufzunehmen, die zusätzliche Informationen über das Ereignis enthalten. Klicken Sie auf die Schaltfläche **Token einfügen**, um eine Liste der verfügbaren Token anzuzeigen. Die Liste enthält eine Kurzbeschreibung für jeden Token.

Sie können Vorlagen bearbeiten, um den Inhalt und das Format von Benachrichtigungs-E-Mails anzupassen. Die Änderungen an den Vorlagen sind benachrichtigungsspezifisch und ereignisspezifisch: Wenn Sie die Vorlage für ein bestimmtes Ereignis innerhalb der Konfiguration einer bestimmten Benachrichtigung ändern, haben Ihre Änderungen keine Auswirkungen auf andere Benachrichtigung oder Ereignisse. Dies ermöglicht, dass unterschiedliche Benachrichtigungen und Ereignisse über verschiedene, benutzerdefinierte Benachrichtigungsvorlagen verfügen.

Gehen Sie folgendermaßen vor, um eine Benachrichtigung anzuzeigen oder zu ändern:

1. Wählen Sie einen Eintrag aus der Liste im Bereich **Ereignisse, Empfänger und Nachrichten** aus und klicken Sie dann auf **Bearbeiten**.
2. Verwenden Sie das Dialogfeld **Benachrichtigungseinstellungen** wie weiter oben in diesem Abschnitt beschrieben.

Gehen Sie folgendermaßen vor, um eine Benachrichtigung zu löschen:

- Wählen Sie den entsprechenden Eintrag aus der Liste im Bereich **Ereignisse, Empfänger und Nachrichten** aus und klicken Sie dann auf **Entfernen**.

ActiveRoles Server Web-Interface

Die in diesem Bereich angegebene Adresse (URL) wird verwendet, um Hyperlinks in den Benachrichtigungsmeldungen zu erstellen, sodass die Benachrichtigungsempfänger leicht auf Web-Interface-Seiten für die Durchführung von Arbeitsablaufaufgaben zugreifen können.

Gehen Sie folgendermaßen vor, um die Adresse des ActiveRoles Server Web-Interface anzugeben:

1. Geben Sie im Bearbeitungsfeld unter **ActiveRoles Server Web-Interface** die Adresse (URL) der ActiveRoles Server Web-Interface-Seite ein (zum Beispiel http://<Server>/ARServerSelfService).
2. Klicken Sie auf **Test**, um die Adresse zu überprüfen. Wenn die Adresse richtig ist, öffnet sich die Web-Interface-Seite in Ihrem Webbrowser.

E-Mail-Servereinstellungen

Die in diesem Bereich angegebenen Einstellungen legen den für die Benachrichtigungsübermittlung zu verwendenden Server fest.

Gehen Sie folgendermaßen vor, um die E-Mail-Servereinstellungen zu konfigurieren:

1. Klicken Sie im Bereich **E-Mail-Servereinstellungen** auf **Eigenschaften**.
2. Verwenden Sie das Dialogfeld **Eigenschaften**, um die E-Mail-Servereinstellungen anzuzeigen oder zu ändern.

Gehen Sie folgendermaßen vor, um eine andere E-Mail-Serverkonfiguration auszuwählen:

- Klicken Sie in der Liste **Konfiguration des Servers für ausgehende Nachrichten** auf den Namen der gewünschten Konfiguration.

Gehen Sie folgendermaßen vor, um eine E-Mail-Serverkonfiguration zu erstellen:

- Erweitern Sie in der ActiveRoles Server-Konsolenstruktur **Configuration | Server configuration**, klicken Sie dann mit der rechten Maustaste auf **E-Mail-Konfiguration** und wählen Sie **Neu | E-Mail-Konfiguration**.

Konfigurieren einer Wenn-Dann-Sonst-Aktivität

Eine Wenn-Dann-Sonst-Aktivität ist eine zusammengesetzte Aktivität. Sie besteht aus mehreren Zweigen. Für jeden dieser Zweige sind individuelle Bedingungen angegeben. Ein Wenn-Dann-Sonst-Zweig kann eine beliebige Anzahl anderer Aktivitäten enthalten. Jeder Vorgang, der die für einen bestimmten Zweig angegebenen Bedingungen erfüllt, führt dazu, dass ActiveRoles Server die in diesem Zweig enthaltenen Aktivitäten ausführt. Es kann nur ein Zweig einer einzelnen Wenn-Dann-Sonst-Aktivität ausgeführt werden, selbst wenn der Vorgang die Bedingungen von mehr als einem Zweig erfüllt.

Normalerweise hat eine Wenn-Dann-Sonst-Aktivität zwei Zweige, wobei für den ersten (äußersten linken) Zweig bestimmte Bedingungen angegeben sind. Für den zweiten Zweig sind keine Bedingungen angegeben, sodass er als der „Sonst"-Zweig fungiert. Wenn ein Vorgang die Bedingungen erfüllt, werden die im ersten Zweig enthaltenen Aktivitäten ausgeführt; andernfalls führt der Vorgang die im zweiten Zweig gefundenen Aktivitäten aus.

Die Konfiguration einer Wenn-Dann-Sonst-Aktivität umfasst die folgenden Aufgaben:

- Hinzufügen eines Zweigs
- Hinzufügen von Aktivitäten zu einem Zweig
- Konfigurieren von Bedingungen für einen Zweig

Gehen Sie folgendermaßen vor, um einen Zweig zu einer Wenn-Dann-Sonst-Aktivität hinzuzufügen:

1. Erweitern Sie in der ActiveRoles Server-Konsolenstruktur **Configuration | Policies | Workflow** und wählen Sie dann den Arbeitsablauf, der die Wenn-Dann-Sonst-Aktivität enthält, die Sie konfigurieren möchten.

   Hierdurch wird das Workflow Designer-Fenster im Bereich „Details" geöffnet, das die Arbeitsablaufdefinition als ein Prozessdiagramm darstellt.

2. Klicken Sie im Prozessdiagramm mit der rechten Maustaste auf den Namen der Wenn-Dann-Sonst-Aktivität und klicken Sie dann auf **Zweig hinzufügen**.

Hierdurch wird ein Zweig mit dem Standardnamen „Wenn-Dann-Sonst-Zweig" hinzugefügt. Klicken Sie mit der rechten Maustaste auf den Namen des Zweigs und klicken Sie dann auf **Eigenschaften**, um den Namen wie gewünscht zu ändern. Sie können einen Zweig löschen, indem Sie auf seinen Name und dann auf **Löschen** klicken.

Gehen Sie folgendermaßen vor, um eine Aktivität zu einem Wenn-Dann-Sonst-Zweig hinzuzufügen:

- Ziehen Sie die Aktivität vom linken Bereich auf den Zweig.

Wenn Sie eine Aktivität zum oberen Teil des Diagramms hinzufügen (über der Zeile **Vorgangs-ausführung**), dann wird die Aktivität in der Vorausführungsphase der Vorgangsverarbeitung ausgeführt (siehe „Übersicht über die Arbeitsablaufverarbeitung" weiter oben in diesem Kapitel). Bestimmte Aktivitäten wie etwa eine Benachrichtigungsaktivität, die für eine Aufführung in der Nachausführungsphase konzipiert sind, können nicht zum oberen Teil des Diagramms hinzugefügt werden.

Wenn Sie eine Aktivität zum unteren Teil des Diagramms hinzufügen (unter der Zeile **Vorgangs-ausführung**), dann wird die Aktivität in der Nachausführungsphase der Vorgangsverarbeitung ausgeführt. Bestimmte Aktivitäten wie etwa eine Genehmigungsaktivität, die für eine Aufführung in der Vorausführungsphase konzipiert sind, können nicht zum unteren Teil des Diagramms hinzugefügt werden.

Sie können eine Aktivität von einem Zweig löschen, indem Sie den Namen der Aktivität und dann auf **Löschen** klicken.

Konfigurieren von Bedingungen für einen Wenn-Dann-Sonst-Zweig

Zweigbedingungen können auf den Eigenschaften der Objekte beruhen, die an der Vorgangsanforderung beteiligt sind. Alternativ kann auch ein Skript verwendet werden, um komplexe Bedingungen zu implementieren.

Gehen Sie folgendermaßen vor, um Zweigbedingungen auf der Grundlage von Objekteigenschaften zu konfigurieren:

1. Klicken Sie mit der rechten Maustaste auf den Namen des Zweigs und klicken Sie dann auf **Eigenschaften**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen** und klicken Sie dann auf die entsprechende Option (die Liste der verfügbaren Optionen ist von dem in den Arbeitsablauf-Startbedingungen angegebenen Vorgangstyp abhängig):
   - Klicken Sie auf **Initiator**, um eine Bedingung auf der Grundlage der Eigenschaften des Vorgangsanforderers hinzuzufügen.
   - Klicken Sie auf **Vorgangsziel**, um eine Bedingung auf der Grundlage der Eigenschaften des Zielobjekts des Vorgangs hinzuzufügen.
   - Klicken Sie auf **Neues Objekt** oder **Geänderte Eigenschaft**, um eine Bedingung auf der Grundlage von Eigenschaften hinzuzufügen, die der Vorgang festlegen oder ändern soll.
   - Klicken Sie auf **Quellcontainer**, um eine Bedingung auf der Grundlage von Eigenschaften des Containers hinzuzufügen, aus dem der Vorgang ein Objekt verschieben wird.
   - Klicken Sie auf **Zielcontainer**, um eine Bedingung auf der Grundlage von Eigenschaften des Containers hinzuzufügen, in den der Vorgang ein Objekt verschieben wird.
3. Verwenden Sie das Dialogfeld **Bedingung konfigurieren**, um die Bedingung einzurichten:
   a) Klicken Sie auf die Schaltfläche **Eigenschaft** und wählen Sie die Eigenschaft aus, die die Bedingung prüfen soll.
   b) Klicken Sie im Bereich **Operator** auf die gewünschte Bedingungsvariable und geben Sie dann im Feld **Wert** einen Eigenschaftswert ein – die Bedingung wird als erfüllt betrachtet, wenn die ausgewählte Eigenschaft mit dem von Ihnen angegebenen Operator/Wert-Paar übereinstimmt.
   c) Klicken Sie auf **OK**.
4. Um weitere Bedingungen hinzuzufügen, wiederholen Sie die Schritte 2-3.

   Sie können mehrere Bedingungen hinzufügen. In diesem Fall werden die Bedingungen per UND zusammengeführt, was bedeutet, dass der Zweig nur dann ausgeführt wird, wenn alle Bedingungen erfüllt sind. Sie können den Operator UND in ODER ändern, indem Sie auf den Eintrag UND in der Liste der Bedingungen doppelklicken.
5. Klicken Sie nach dem Konfigurieren der Bedingungen auf **OK**, um das Dialogfeld **Eigenschaften** zu schließen.

Skriptbasierte Bedingungen

Um eine skriptbasierte Bedingung zu implementieren, müssen Sie ein Skriptmodul erstellen und anwenden, das eine Funktion enthält, die den angeforderten Vorgang analysiert, um zu ermitteln, ob der Zweig ausgeführt werden soll oder nicht. Die Funktion kann den ADSI-Provider von ActiveRoles Server verwenden, um auf die Eigenschaften der am Vorgang beteiligten Objekte zuzugreifen, um die Eigenschaften zu analysieren und um dann abhängig von den Ergebnissen der Analyse den Wert TRUE oder FALSE auszugeben. Der Zweig wird ausgeführt, wenn die Funktion TRUE ausgibt.

Gehen Sie folgendermaßen vor, um die skriptbasierte Bedingung anzuwenden:

1. Klicken Sie mit der rechten Maustaste auf den Namen des Zweigs und klicken Sie dann auf **Eigenschaften**.
2. Klicken Sie im Dialogfeld **Eigenschaften** auf die Schaltfläche **Hinzufügen** und klicken Sie dann auf **Skript**.
3. Verwenden Sie das Dialogfeld **Skriptbedingung konfigurieren**, um das Skriptmodul auszuwählen und die Funktion anzugeben, die die anzuwendende Bedingung definiert.

Weitere Informationen und Anweisungen finden Sie im Abschnitt „Entwickeln von skriptbedingten Funktionen" in der ActiveRoles Server SDK and Resource Kit-Dokumentation.

Konfigurieren einer Stoppen/Unterbrechen-Aktivität

Bei der Konfiguration einer Stoppen/Unterbrechen-Aktivität können Sie den Text einer Nachricht angeben. Die Aktivität beendet die Arbeitsablaufinstanz und meldet das entsprechende Ereignis an das „EDM-Server"-Ereignisprotokoll. Die Nachricht ist in der Ereignisbeschreibung enthalten. Falls möglich zeigt die Aktivität auch die Nachricht in der Client-Benutzeroberfläche (wie etwa in der ActiveRoles Server-Konsole oder im Web-Interface) an, von der aus der Vorgang, der die Arbeitsablaufinstanz gestartet hat, initiiert wurde.

Gehen Sie folgendermaßen vor, um eine Stoppen/Unterbrechen-Aktivität zu konfigurieren:

1. Erweitern Sie in der ActiveRoles Server-Konsolenstruktur **Configuration | Policies | Workflow** und wählen Sie dann den Arbeitsablauf, der die Stoppen/Unterbrechen-Aktivität enthält, die Sie konfigurieren möchten.

   Hierdurch wird das Workflow Designer-Fenster im Bereich „Details" geöffnet, das die Arbeitsablaufdefinition als ein Prozessdiagramm darstellt.
2. Klicken Sie im Prozessdiagramm mit der rechten Maustaste auf den Namen der Aktivität und klicken Sie dann auf **Eigenschaften**.
3. Zeigen Sie den Nachrichtentext an und ändern Sie ihn erforderlichenfalls.

Aktivieren oder Deaktivieren eines Arbeitsablaufs

Die temporäre Deaktivierung eines Arbeitsablaufs kann nützlich sein, wenn an dem Arbeitsablauf gearbeitet wird, sodass die Arbeitsablaufdefinition noch nicht abgeschlossen ist und die im Arbeitsablauf enthaltenen Aktivitäten bis zu einem späteren Zeitpunkt nicht ausgeführt werden sollen.

Gehen Sie folgendermaßen vor, um einen Arbeitsablauf zu deaktivieren bzw. um einen deaktivierten Arbeitsablauf zu aktivieren:

- Klicken Sie mit der rechten Maustaste auf den Arbeitsablauf und klicken Sie dann auf **Arbeitsablauf deaktivieren** bzw. **Arbeitsablauf aktivieren**.

Wenn ein Arbeitsablauf deaktiviert ist, passt der Verwaltungsdienst den Arbeitsablauf unabängig davon, ob ein Vorgang die Arbeitsablauf-Startbedingungen erfüllt oder nicht, keinem Vorgang an. Als Folge werden die in einem deaktivierten Arbeitsablauf enthaltenen Aktivitäten niemals ausgeführt. Wenn Sie einen deaktivierten Arbeitsablauf aktivieren, erlauben Sie dem Verwaltungsdienst die Ausführung der in diesem Arbeitsablauf gefundenen Aktivitäten.

Beispiel: Genehmigungs-Arbeitsablauf

Der Genehmigungs-Arbeitsablauf ergänzt die automatisierten Richtlinien, um Bereitstellungs- und Deprovisionsentscheidungen auf der Grundlage von Eingaben durch den Menschen zu treffen. Während automatisierte Richtlinien keinen manuellen Eingriff erfordern, erweitert die auf Genehmigungen basierende Durchführung administrativer Vorgänge die Prozessautomatisierung um die Möglichkeit, Vorgangsanforderungen manuell zu akzeptieren oder zurückzuweisen und die Ausführung von anforderungsverarbeitenden Aufgaben zu überwachen, um zu gewährleisten, dass diese zeitnah beantwortet werden.

Der Genehmigungs-Arbeitsablauf kann für eine Vielzahl von Anforderungen genutzt werden. Bei diesen Anforderungen handelt es sich um Benutzervorgänge, die zur Durchführung von Verwaltungsvorgängen dienen. Als Beispiel für derartige Vorgänge seien hier nur die Erstellung, Änderung und Deprovisionierung von Benutzerkonten genannt.

Wenn ein angeforderter Vorgang die Berechtigung durch bestimmte Personen in einer Organisation erfordert, kann ein Arbeitsablauf zur Koordination des Genehmigungsprozesses gestartet werden. Das System führt den angeforderten Vorgang erst durch, wenn eine autorisierte Person die entsprechende Genehmigung erteilt hat.

ActiveRoles Server-Administratoren können Genehmigungs-Arbeitsabläufe mit Hilfe von Workflow Designer – einem grafischen Tool, das in der ActiveRoles Server-Konsole für die Erstellung von Arbeitsabläufen bereitgestellt wird – erstellen und konfigurieren. Beim Entwurf eines Genehmigungs-Arbeitsablaufs gibt der Administrator an, welche Art von Vorgang zum Start des Arbeitsablaufs führt, und fügt Genehmigungsregeln zum Arbeitsablauf hinzu. Die Genehmigungsregeln legen fest, wer autorisiert ist, den Vorgang zu genehmigen. Sie legen außerdem die erforderliche Reihenfolge der Genehmigungen und die Personen, die über Genehmigungsaufgaben oder Entscheidung informiert werden sollen, fest.

Die von ActiveRoles Server bereitgestellte, auf einem Genehmigungs-Arbeitsablauf basierende Bereitstellungslösung umfasst die folgenden Komponenten:

- Der Workflow Designer für die Erstellung von Arbeitsabläufen, der in der ActiveRoles Server-Konsole verfügbar ist. Verwenden Sie den Workflow Designer, um einen Genehmigungs-Arbeitsablauf durch Hinzufügen von Genehmigungsaktivitäten zur Arbeitsablaufdefinition zu konfigurieren.
- Die Verzeichnisverwaltungsschnittstellen wie etwa das Web-Interface oder die ActiveRoles Server-Konsole für das Senden von Vorgangsanforderungen zur Genehmigung. Der Genehmigungs-Arbeitsablauf kann beispielsweise so konfiguriert werden, dass die Erstellung eines Benutzerkontos über ActiveRoles Server den Genehmigungs-Arbeitsablauf startet, anstatt sofort die Benutzererstellung zu beginnen.
- Der mit der Genehmigung zusammenhängende Bereich des Web-Interface für die Verwaltung von Vorgangsanforderungen. Dieser Bereich enthält eine Aufgabenliste für die Genehmigungsaufgaben, die ein festgelegter Benutzer ausführen muss. Diese Liste ermöglicht es dem Benutzer, Aufgaben wie etwa das Genehmigen oder Zurückweisen von Vorgangsanforderungen auszuführen.

Begriffsdefinition

In diesem Abschnitt sind einige wichtige, für den Genehmigungs-Arbeitsablauf geltende Definitionen zusammengefasst.

Benachrichtigung

Die Mittel, die für die Benachrichtigung eines Benutzers oder einer Gruppe von Benutzern über eine bestimmte vordefinierte Situation, die sich innerhalb eines Arbeitsablaufs ergeben kann verwendet werden. Eine Benachrichtigungsmeldung wird generiert und per E-Mail an die angegebenen Empfänger gesendet, um sie über den Eintritt eines bestimmten Ereignisses wie etwa das Senden einer neuen Genehmigungsaufgabe an die genehmigenden Instanzen oder den Abschluss des Vorgangs zu informieren. Eine Benachrichtigungskonfiguration, gespeichert als Teil einer Genehmigungsregel, umfasst solche Elemente wie etwa das Ereignis, bei dessen Eintritt eine Benachrichtigung erfolgen soll, die Liste der Benachrichtigungsempfänger und die Vorlage für die Benachrichtigungsmeldung. ActiveRoles Server bietet zusätzlich zu Genehmigungsregeln noch eine separate Arbeitsablauf-Aktivitätskategorie zum Zwecke der Benachrichtigung.

Genehmigung

Ein Entscheidungspunkt in einem Arbeitsablauf, der verwendet wird, um vor dem Fortsetzen des Arbeitsablaufs die Genehmigung von einer Person zu erhalten.

Genehmigungsregel (Genehmigungsaktivität)

Arbeitsablaufaktivitäten der Kategorie „Genehmigung" werden als „Genehmigungsregeln" bezeichnet. Die Arbeitsablauf-Startbedingungen geben an, welche Vorgänge den Arbeitsablauf starten. Die zum Arbeitsablauf hinzugefügten Genehmigungsregeln bestimmen, wer den Vorgang genehmigen darf, in welcher Reihenfolge die Genehmigungen erfolgen sollen und wer über Genehmigungsaufgaben oder Entscheidungen benachrichtigt werden soll.

Genehmigungsaufgabe

Eine als Teil der Verarbeitung einer Genehmigungsregel erstellte und einer genehmigenden Instanz zugewiesene Aufgabe. Von der genehmigenden Instanz wird die Erfüllung der Aufgabe erwartet, d. h. sie muss die Entscheidung treffen, ob der Vorgang zulässig ist oder abgelehnt werden soll.

Genehmigende Instanz

Die für die Durchführung einer Genehmigungsaufgabe bestimmte Person. Die Einstellung, die die genehmigenden Instanzen festlegt, ist ein Konfigurationselement einer Genehmigungsregel. Bei der Verarbeitung einer Genehmigungsregel erstellt ActiveRoles Server eine Genehmigungsaufgabe und weist sie dann den von der Regel definierten genehmigenden Instanzen zu. Der Status der Aufgabe bestimmt den Übergang des Arbeitsablaufs: die Aufgabe muss die Auflösung „Genehmigen" erhalten, damit der Vorgang der Genehmigungsregel entspricht. Wenn der Aufgabe die Auflösung „Zurückweisen" zugewiesen wird, wurde der Vorgang verweigert, und die Arbeitsablaufinstanz ist abgeschlossen.

Initiator (Anforderer)

Die Identität des Benutzers oder Dienstes, der einen Vorgang in ActiveRoles Server angefordert hat. Wenn zum Beispiel die ActiveRoles Server-Konsole verwendet wird, um ein Objekt zu ändern oder zu erstellen, wird der Konsolenbenutzer als der Initiator des entsprechenden Vorgangs identifiziert. Der Initiator eines Vorgangs wird auch als „Vorgangsanforderer" bezeichnet.

Vorgang

Eine Anforderung für bestimmte, an Verzeichnisdaten vorzunehmende Änderungen wie etwa die Erstellung von Benutzern oder das Hinzufügen von Benutzern zu Gruppen. Ein Vorgang kann einen Genehmigungs-Arbeitsablauf starten. In diesem Fall werden die angeforderten Änderungen nur durchgeführt, nachdem sie genehmigt wurden.

Zielobjekt des Vorgangs

Das vom Vorgang zu ändernde oder zu erstellende Objekt. Wenn beispielsweise die Erstellung eines Benutzerkontos angefordert wird, wird das Konto als „Zielobjekt des Vorgangs" bezeichnet. Bei einer Anforderung zum Hinzufügen eines Benutzers zu einer Gruppe wird die Gruppe als das „Zielobjekt des Vorgangs" bezeichnet.

Funktionsweise

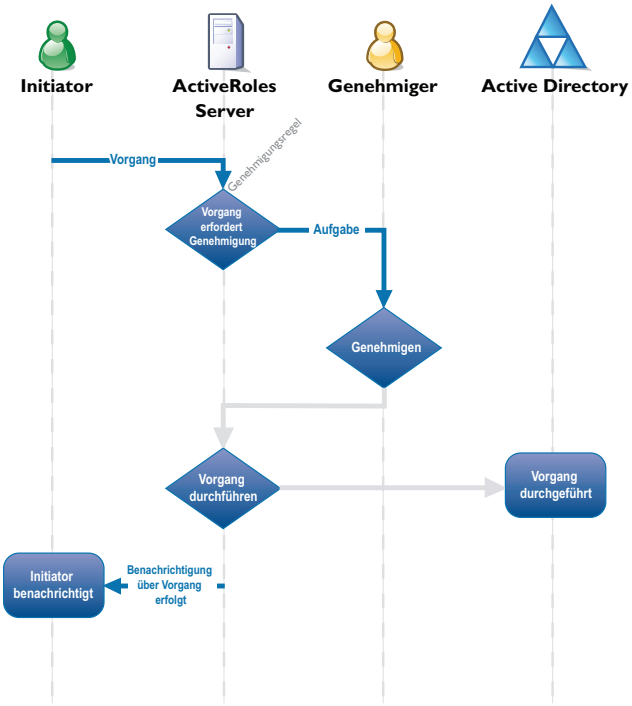
Der Genehmigungs-Arbeitsablauf wird durch Arbeitsablauf-Startbedingungen und Genehmigungsregeln gesteuert. Arbeitsablauf-Startbedingungen legen fest, welche Art von Vorgang den Start des Arbeitsablaufs bewirkt. Die zum Arbeitsablauf hinzugefügten Genehmigungsregeln legen die Personen fest, die autorisiert sind, den Vorgang zu genehmigen (genehmigende Instanzen).

Wenn ein ActiveRoles Server-Benutzer einen Vorgang anfordert, führt ActiveRoles Server eine Überprüfung durch, um zu ermitteln, ob der Vorgang den Startbedingungen eines Arbeitsablaufs entspricht, und startet dann den Arbeitsablauf, dessen Bedingungen erfüllt sind. Eine im Arbeitsablauf enthaltene Genehmigungsregel generiert dann eine Genehmigungsaufgabe und weist sie den von der Regel definierten genehmigenden Instanzen zu.

Eine genehmigende Instanz schließt eine Genehmigungsaufgabe ab, indem Sie die Aktion „Genehmigen" oder „Zurückweisen" auf die Aufgabe anwendet. Hierdurch ändert sich der Status der Aufgabe von „Ausstehend" in „Genehmigt" bzw. „Zurückgewiesen".

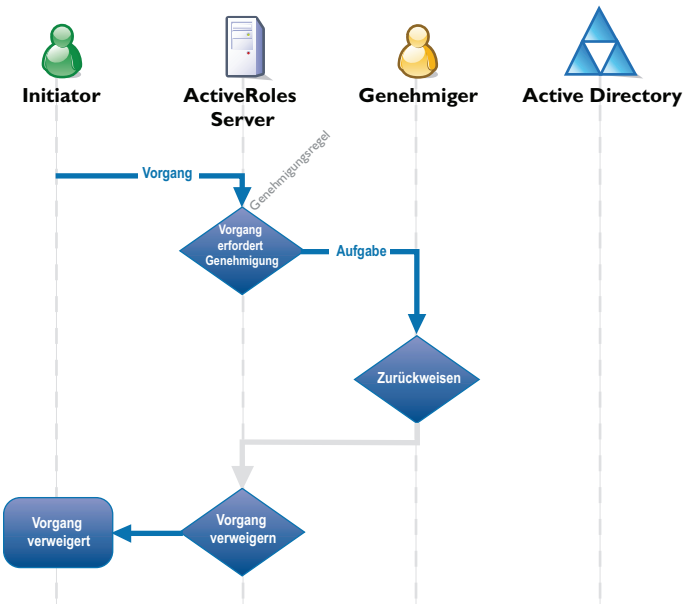
Vorgang: Genehmigen

Wenn die genehmigende Instanz den Vorgang „Genehmigen" auf die Aufgabe anwendet, ermöglicht ActiveRoles Server die Durchführung des Vorgangs:



Vorgang: Zurückweisen

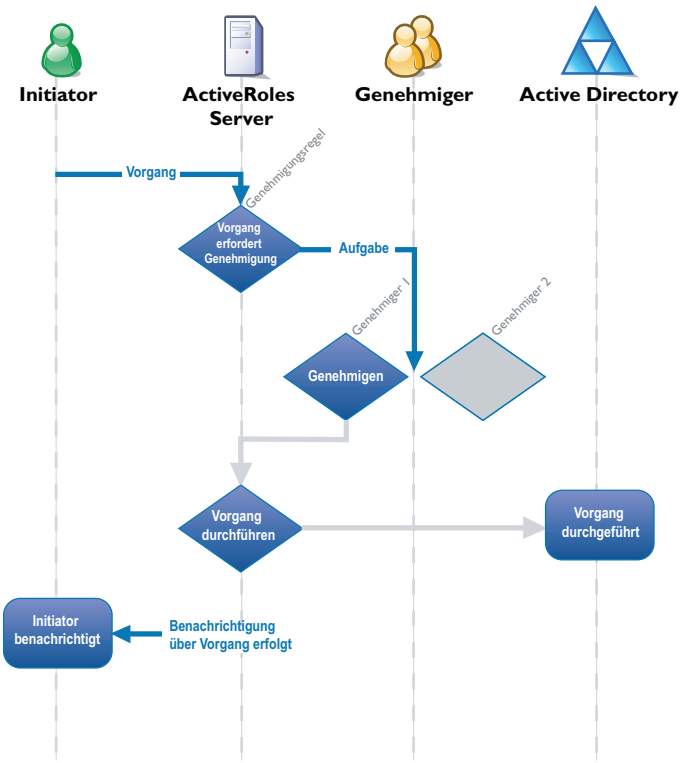
Wenn der Genehmiger den Vorgang „Zurückweisen" auf die Aufgabe anwendet, bricht ActiveRoles Server den Vorgang ab:



Mehrere Genehmigungsstellen

Eine Genehmigungsregel kann so konfiguriert werden, dass eine einzelne Aufgabe mehreren Genehmigungsstellen zugeordnet wird. So kann zum Beispiel eine Gruppe als eine genehmigende Instanz bestimmt werden, was dazu führt, dass die Aufgabe jedem Mitglied der Gruppe zugewiesen wird. In diesem Fall schließt der erste der Genehmiger, der den Vorgang „Genehmigen" oder „Zurückweisen" auf die Aufgabe anwendet, die Aufgabe ab.

Wenn der Vorgang „Genehmigen" auf die Aufgabe angewendet wird, ermöglicht ActiveRoles Server die Durchführung des Vorgangs. Wenn der Vorgang „Zurückweisen" auf die Aufgabe angewandt wird, bricht ActiveRoles Server den Vorgang ab.

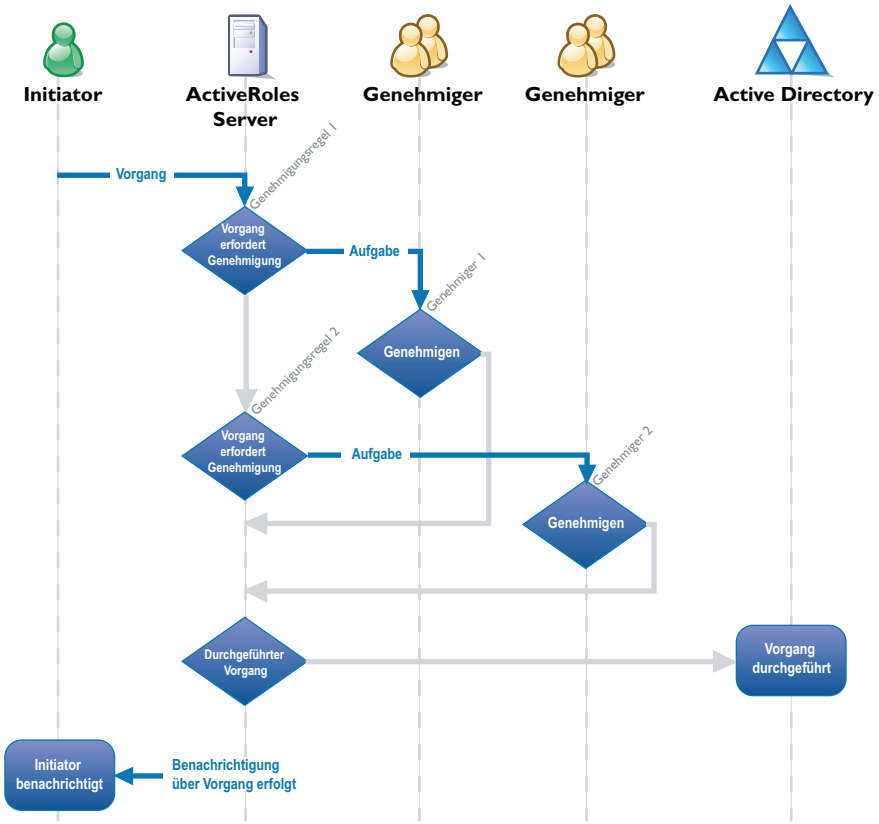


Mehrere Aufgaben

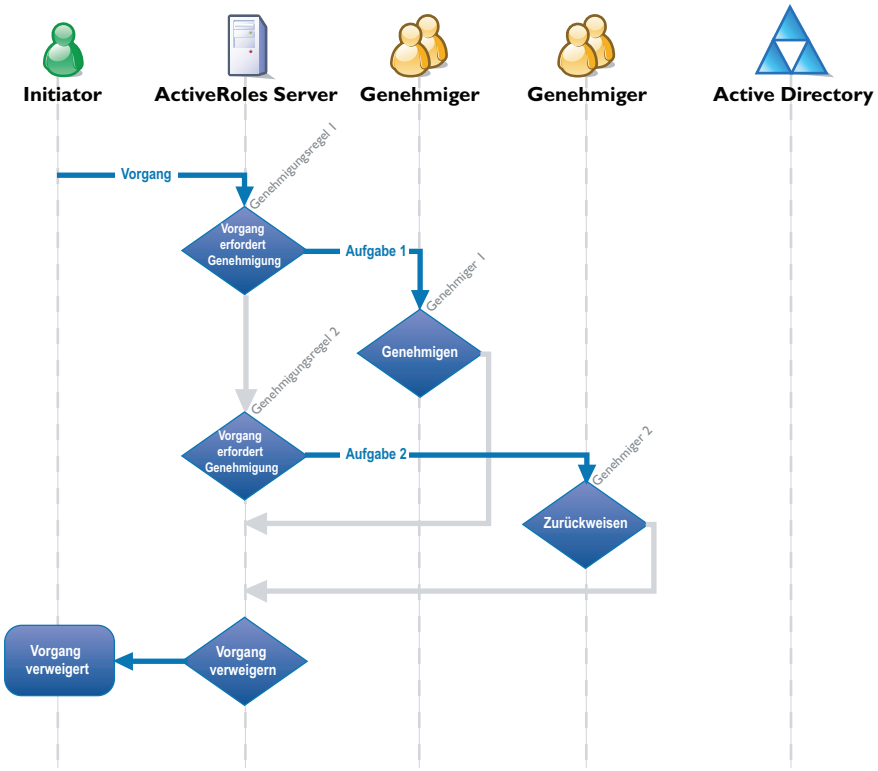
Die Anzahl der von einer einzigen Arbeitsablaufinstanz generierten Genehmigungsaufgaben hängt davon ab, wie viele Genehmigungsregeln im Arbeitsablauf enthalten sind (eine Aufgabe je Regel). Daher werden, wenn ein Arbeitsabläufe mehrere Genehmigungsregeln enthält, mehrere Aufgaben erstellt und den entsprechenden genehmigenden Instanzen zugewiesen.

Innerhalb eines einzelnen Arbeitsablaufs werden Genehmigungsregeln nacheinander (sequenziell) angewandt. Das bedeutet, dass eine nachfolgende Regel nur angewandt wird, wenn der angeforderte Vorgang der vorherigen Regel entspricht.

Wenn der Vorgang „Genehmigen" auf alle Aufgabe angewendet wird, ermöglicht ActiveRoles Server die Durchführung des Vorgangs.



Wenn auf mindestens eine der Aufgaben der Vorgang „Zurückweisen" angewandt wird, bricht ActiveRoles Server den Vorgang ab:



Erstellen und Konfigurieren eines Genehmigungs-Arbeitsablaufs

Um ein Genehmigungsszenario zu implementieren, in dem bestimmte Vorgänge die Genehmigung in ActiveRoles Server erfordern, erstellen Sie eine Arbeitsablaufdefinition, konfigurieren dann die Arbeitsablauf-Startbedingungen, fügen Genehmigungsaktivitäten (Genehmigungsregeln) hinzu und konfigurieren diese Ihren Anforderungen entsprechend. All diese Aufgaben werden mit Hilfe von Workflow Designer – einem in der ActiveRoles Server-Konsole enthaltenen grafischen Tool – durchgeführt.

Bei der Konfiguration von Arbeitsablauf-Startbedingungen geben Sie Folgendes an:

- Vorgangstyp wie etwa Erstellen, Umbenennen, Ändern oder Löschen; der Arbeitsablauf startet nur dann, wenn ein Vorgang dieses Typs angefordert wird.
- Objekttyp wie etwa Benutzer, Gruppe oder Computer; der Arbeitsablauf startet nur dann, wenn der Vorgang Änderungen an einem Objekt dieses Typs anfordert.
- Für den Vorgangstyp „Ändern" eine Liste der Objekteigenschaften; der Arbeitsablauf startet nur dann, wenn der Vorgang Änderungen an irgendeiner dieser Eigenschaften eines Objekts anfordert.
- Identität eines Vorgangsanforderers (Initiator) wie etwa ein Benutzer, eine Gruppe oder ein Dienst; der Arbeitsablauf startet nur dann, wenn der Vorgang im Namen dieser Identität angefordert wird.

- Container wie etwa eine Organisationseinheit oder eine verwaltete Einheit; der Arbeitsablauf startet nur dann, wenn der Vorgang Änderungen an bzw. die Erstellung von einem Objekt in diesem Container anfordert.
- Optional ein Filter, der alle zusätzlichen Bedingungen für die an einem Vorgang beteiligten Einheiten definiert; Der Arbeitsablauf startet nur dann, wenn der Vorgang diesen Bedingungen entspricht. Wenn kein Filter festgelegt ist, dann sind keine zusätzlichen Bedingungen gültig.

Jeder Vorgang, der alle für einen Arbeitsablauf angegebenen Startbedingungen erfüllt, führt zum Start des Arbeitsablaufs.

Bei der Konfiguration einer Genehmigungsregel innerhalb eines Arbeitsablaufs geben Sie Folgendes an:

- Eine Liste der genehmigenden Instanzen wie etwa Benutzer oder Gruppen; diese Einstellung gibt die Personen an, die autorisiert sind, Vorgänge zuzulassen oder zu verweigern, die den Arbeitsablauf starten.
- Benachrichtigungseinstellungen wie etwa Arbeitsablaufereignisse, bei deren Eintreten eine Benachrichtigung erfolgen soll, Benachrichtigungsempfänger, Übermittlungsoptionen und die Benachrichtigungsmeldungsvorlage.

Erstellen einer Arbeitsablaufdefinition

Die ActiveRoles Server-Konsole enthält den Workflow Designer zum Erstellen und Konfigurieren von Arbeitsabläufen. Zunächst erstellen Sie eine Arbeitsablaufdefinition. Verwenden Sie dann Workflow Designer, um den Arbeitsablauf zu erstellen, indem Sie Arbeitsablaufaktivitäten hinzufügen und jegliche andere erforderliche Änderungen an der Arbeitsablaufdefinition vornehmen.

Schrittweise Anweisungen finden Sie im Abschnitt „Erstellen einer Arbeitsablaufdefinition" weiter oben in diesem Kapitel.

Angeben von Arbeitsablauf-Startbedingungen

Sie können die Startbedingungen für einen Arbeitsablauf festlegen, indem Sie seine Definition im Workflow Designer bearbeiten. Die Startbedingungen legen fest, welche Vorgänge zum Start des Arbeitsablaufs führen.

Schrittweise Anweisungen finden Sie im Abschnitt „Konfigurieren der Startbedingungen für einen Arbeitsablauf" weiter oben in diesem Kapitel.

Beispiel Angenommen, Sie möchten, dass die Erstellung von Benutzerkonten in einer bestimmten Organisationseinheit eine Genehmigung erfordert. Sie können dieses Szenario implementieren, indem Sie die Arbeitsablauf-Startbedingungen wie folgt konfigurieren:

- Setzen Sie den Vorgangstyp auf ‚Erstellen'.
- Setzen Sie den Objekttyp auf ‚Benutzer'.
- Setzen Sie den Initiator auf ‚Jeder beliebige Benutzer'.
- Legen Sie den Container fest, indem Sie die gewünschte Organisationseinheit auswählen.

Als Ergebnis dieser Bedingungen startet der Arbeitsablauf immer dann, wenn ActiveRoles Server für die Erstellung eines Benutzerkontos in dieser Organisationseinheit verwendet wird.

Festlegen der Genehmiger

Bei der Erstellung eines Genehmigungs-Arbeitsablaufs fügen Sie ein oder mehrere Genehmigungsaktivitäten zur Arbeitsablaufdefinition hinzu und erstellen so Genehmigungsregeln. Anschließend konfigurieren Sie Aktivitäten, um die genehmigenden Instanzen für jede Regel zu definieren. Die Organe, die als genehmigende Instanzen festgelegt werden können, umfassen den Verwalter des Vorgangsanforderers, den Verwalter des Zielobjekts des Vorgangs und den Verwalter des Containers, in dem sich das Zielobjekt des Vorgangs befindet. Es ist auch möglich, jeden beliebigen Benutzer oder jede beliebige Benutzergruppe für die Funktion für genehmigenden Instanz auszuwählen.

Beispiel Wir erweitern das vorige Beispiel und nehmen an, dass die Erstellung von Benutzerkonten von dem Verwalter der Organisationseinheit genehmigt werden muss, in der die Konten erstellt werden sollen. Sie können dieses Szenario implementieren, indem Sie eine Genehmigungsaktivität zum Arbeitsablauf hinzufügen und dann den Befehl **Eigenschaften** auf diese Aktivität anwenden, um die entsprechende Option auf der Seite **Genehmigende Instanzen bestimmen** auszuwählen.

Schrittweise Anweisungen finden Sie im Abschnitt „Konfigurieren einer Genehmigungsaktivität" weiter oben in diesem Kapitel.

Konfigurieren von Benachrichtigungen

Sie können Genehmigungsregeln konfigurieren, um genehmigende Instanzen oder andere interessierte Parteien über bestimmte Ereignisse zu informieren, die während des Genehmigungsprozesses eintreten können. So kann zum Beispiel eine Genehmigungsregel so konfiguriert werden, dass die durch die Regel festgelegten genehmigenden Instanzen immer dann eine E-Mail-Benachrichtigung erhalten, wenn ein Vorgang angefordert wird, der ihre Genehmigung erfordert. Zu den weiteren Ereignissen, bei deren Eintritt eine Benachrichtigung erfolgen soll, gehört der Abschluss einer Genehmigungsaufgabe. Diese Benachrichtigungen geben an, dass eine genehmigende Instanz die angeforderten Änderungen entweder genehmigt oder verweigert hat. Der Abschluss des Vorgangs gibt an, dass die angeforderten Änderungen angewandt wurden, und das Fehlschlagen eines Vorgangs bedeutet, dass eine Fehlerbedingung vorliegt.

Benachrichtigungsempfänger

Bei der Konfiguration von Benachrichtigungseinstellungen in einer Genehmigungsregel wählen Sie ein Ereignis aus und geben an, wer eine E-Mail-Benachrichtigung bezüglich des Ereignisses erhalten soll (die Benachrichtigungsempfänger). Ein Empfänger kann jeder beliebige Postfach-fähige Benutzer oder jede E-Mail-fähige Gruppe sein. Es gibt auch eine Reihe von Optionen, die es Ihnen ermöglichen, Empfänger auf der Grundlage ihrer Funktion wie etwa ein Vorgangsanforderer, eine genehmigende Instanz, ein Verwalter des Vorgangsanforderers oder ein Verwalter des Zielobjekts des Vorgangs auszuwählen. Es kann eine einzelne Regel konfiguriert werden, um eine Benachrichtigen bezüglich eines oder mehrerer Ereignisse zu senden, wobei eine individuelle Empfängerliste für jedes Ereignis definiert werden kann.

Benachrichtigungsübermittlung

Zusammen mit der Auswahl des Ereignisses, bei dessen Eintritt eine Benachrichtigung erfolgen soll, und der Benachrichtigungsempfänger können Sie auch Übermittlungsoptionen auswählen. Zusätzlich zur sofortigen Übermittlung (was dazu führt, dass bei jedem Eintritt des Ereignisses eine separate Benachrichtigungsmeldung generiert wird) gibt es auch die Möglichkeit der geplanten Übermittlung zur Zusammenfassung mehrerer Benachrichtigungen. Wenn sie sich für eine geplante Übermittlung

entschließen, werden alle Benachrichtigungen über den Eintritt des Ereignisses innerhalb eines frei wählbaren Zeitraums gesammelt und als eine einzige Nachricht gesendet. In diesem Fall besteht der Nachrichtentext aus den zusammengefassten Benachrichtigungen über jedes einzelne Eintreten des Ereignisses.

Benachrichtigungsmeldungen werden zur Übermittlung durch einen SMTP-Dienst wie etwa den von Microsoft Exchange oder Internet Information Services bereitgestellten Dienst weitergeleitet. Die Adresse und weitere Parameter des E-Mail-Servers für ausgehende E-Mails werden im Rahmen der Konfiguration der Benachrichtigungseinstellungen für jede Genehmigungsregel angegeben.

Vorlage für Benachrichtigungsmeldungen

Benachrichtigungsmeldungen basieren auf einer Nachrichtenvorlage, die das Format und den Inhalt von E-Mail-Benachrichtigungen einschließlich des Nachrichtenbetreffs und Nachrichtentexts festlegt. Sie können die Vorlage auf der Seite, auf der Sie ein Ereignis zusammen mit den Benachrichtigungs-empfängern auswählen, aufrufen. Wenn Sie die Vorlage ändern, werden die von Ihnen durchgeführten Änderungen nur für die Nachrichten berücksichtigt, die in Zusammenhang mit der von Ihnen konfigurierten Benachrichtigung stehen.

Nachrichtenvorlagen verwenden so genannte Token, um dynamische Inhalt zu Benachrichtigungs-meldungen hinzuzufügen. Sie können Token aus einer Liste auswählen und sie dann zur Nachrichtenvorlage hinzufügen. Jeder Token führt dazu, dass der Nachrichtentext eine bestimmte Informationen anstelle des Tokens enthält. Wenn Sie eine Nachricht generieren, erfasst das System von den Token repräsentierte Informationen und fügt diese Informationen dann in die Nachricht ein.

Beispiel Im vorigen Beispiel können Sie die Genehmigungsaktivität so konfigurieren, dass die genehmigende Instanz immer dann eine E-Mail-Benachrichtigung empfängt, wenn die Erstellung eines Benutzers angefordert wird, die eine Genehmigung erfordert. Öffnen Sie die Seite **Eigenschaften** für diese Aktivität und fahren Sie mit dem Schritt **Benachrichtigung** fort. Klicken Sie dann auf **Hinzufügen**, überprüfen Sie, ob das Ereignis **Aufgabe erstellt** markiert ist, und aktivieren Sie das entsprechende Kontrollkästchen unter **Benachrichtigungsempfänger**.

Schrittweise Anweisungen finden Sie im Abschnitt „Konfigurieren einer Benachrichtigungsaktivität" weiter oben in diesem Kapitel.

8

Temporäre Gruppenmitgliedschaft

- Beschreibung von temporären Gruppenmitgliedschaften
- Verwenden von temporären Gruppenmitgliedschaften

Beschreibung von temporären Gruppenmitgliedschaften

Mit temporären Gruppenmitgliedschaften bietet ActiveRoles Server die Möglichkeit, die Aufgaben des Hinzufügens oder Entfernens von Gruppenmitgliedern, die nur für einen bestimmten Zeitraum eine Gruppenmitgliedschaft benötigen, zu automatisieren. Beim Hinzufügen von Objekten wie etwa Benutzern, Computern oder Gruppen zu einer bestimmten Gruppe kann ein Administrator festlegen, dass die Objekte zum gewählten Zeitpunkt zu der Gruppe hinzugefügt werden sollen. Außerdem kann er angeben, wann diese Objekte aus der Gruppe entfernt werden sollen.

Die von ActiveRoles Server angebotene Funktion der temporären Gruppenmitgliedschaft kann Organisationen bei der effizienten Zuordnung von Benutzern und anderen Objekten zu Gruppen für einen bestimmten Zeitraum unterstützen. Obwohl in vielen Fällen Objekte, die zu einer Gruppe hinzugefügt werden, auf unbestimmte Zeit Mitglieder der Gruppe bleiben, besteht in vielen Organisationen die Notwendigkeit der temporären Zuweisung von Objekten zu bestimmten Gruppen. Zu den typischen Szenarien gehört etwa die Gewährung des Zugriffs auf spezifische Ressourcen für die Dauer eines bestimmten Projekts oder die temporäre Zuweisung der Rolle als ein Serveradministrator.

Die Verwaltung von temporären Gruppenzuweisungen stellt eine besondere Herausforderung für Administratoren dar, da ein hohes Maß an administrativer Übersicht erforderlich ist, um zu gewährleisten, dass die Gruppenzuweisungen wirklich temporär sind und nicht aufgrund einer mangelhaften Kontrolle über die Gruppenmitgliedschaften zu einer permanenten Gruppenzuweisung werden. ActiveRoles Server löst dieses Problem, indem es das Hinzufügen und Entfernen von Gruppenmitgliedern auf einer geplanten Basis automatisiert.

Die Funktion der temporären Gruppenmitgliedschaft erweitert die Vorteile von ActiveRoles Server in den folgenden Bereichen:

- **Sicherheit** Durch die strenge Kontrolle über Änderungen an Gruppenmitgliedschaften einschließlich richtlinienbasierter Regeln und Einschränkungen, Änderungsgenehmigungen und Änderungsüberprüfungen verringert ActiveRoles Server das Sicherheitsrisiko für Systeme, Anwendungen und Dienste, die Active Directory-Gruppen für die Autorisierung des Zugriffs verwenden. Das rechtzeitige Hinzufügen und Entfernen von Gruppenmitgliedern gewährleistet, dass die Benutzer nur für die erforderliche Dauer Zugriff auf System und Ressourcen haben. So werden die Möglichkeit und der Umfang des Zugriffs eingeschränkt.
- **Verfügbarkeit** Durch das automatische Füllen der Gruppen auf der Grundlage von konfigurierbaren Richtlinienregeln macht ActiveRoles Server entsprechende Netzwerkressourcen für die entsprechenden Benutzer genau zu dem Zeitpunkt verfügbar, an dem sie einen Zugriff auf diese Ressourcen benötigen. Die Möglichkeit, einen Zeitplan für das Hinzufügen und Entfernen von Gruppenmitgliedern zu erstellen, ist hilfreich in Situationen, in denen der temporäre Zugriff für eine relativ kurze Dauer erforderlich ist oder wenn kurzfristig zahlreiche Anforderungen zur Änderung der Gruppenmitgliedschaften eintreffen.

- **Verwaltbarkeit** ActiveRoles Server rationalisiert die Zuweisung von Benutzern zu Gruppen sowie das Entfernen von Mitgliedern aus Gruppen. Eine einheitliche und zuverlässige Kontrolle dieser Bereitstellungs- und Deprovisionierungsaktivitäten verringert den Arbeitsaufwand für die Personen, die für die Verwaltung von Active Directory-Gruppen verantwortlich sind. Eine unbeaufsichtigte, auf einer Planung beruhende Handhabung der temporären Gruppenmitgliedschaften trägt zur Gewährleistung der Konformität mit Änderungs- und Zugriffsrichtlinien bei und vereinfacht gleichzeitig die Verwaltung von Gruppenmitgliedschafts-Änderungsanforderungen.
- **Konformität** ActiveRoles Server senkt die Gefahr einer Nichtübereinstimmung mit behördlichen Vorschriften, indem es eine ordnungsgemäße und effektive Kontrolle der Gruppenmitgliedschaften gewährleistet. Da Active Directory-Gruppen verwendet werden, um den Zugriff auf Systeme, Anwendungen und Daten zu autorisieren, trägt die Kontrolle der Zuweisung von Benutzern zu Gruppen auf einer temporären Basis dazu bei, dass die Organisationen die Anforderungen im Hinblick auf die Trennung von Pflichten und den Datenschutz erfüllen.

ActiveRoles Server bietet die Funktion der temporären Gruppenmitgliedschaft sowohl für Active Directory-Domänendienste (AD DS) als auch für Active Directory Lightweight Directory Services (AD LDS).

Die Funktion der temporären Gruppenmitgliedschaft automatisiert die Aufgaben des Hinzufügens und Entfernens von Benutzern zu bzw. aus Gruppen in Situationen, in denen die Benutzer die Gruppenmitgliedschaft nur für einen bestimmten Zeitraum benötigen. Durch Anwendung von Einstellungen für die temporäre Gruppenmitgliedschaft können die Administratoren die Zuweisung von ausgewählten Objekten zu einer bestimmten Gruppe planen und angeben, wann die Objekte aus der Gruppe entfernt werden sollen.

Nachfolgend sind die von ActiveRoles Server zur Verwaltung der temporären Gruppenmitgliedschaften angebotenen Hauptfunktionen aufgeführt:

- **Temporäre Gruppenmitglieder hinzufügen** Die Benutzerschnittstelle für die Auswahl von Objekten, sowohl in der ActiveRoles Server-Konsole als auch im Web-Interface, bietet eine Reihe von Optionen für die Festlegung, wann die ausgewählten Objekte zur ausgewählten Gruppe hinzugefügt werden sollen und wann die ausgewählten Objekte aus der Gruppe entfernt werden sollen. Es ist möglich, die Objekte sofort zur Gruppe hinzuzufügen und anzugeben, dass die Objekte nicht aus der Gruppe entfernt werden sollen.
- **Temporäre Mitglieder einer Gruppe anzeigen** Die von der ActiveRoles Server-Konsole oder vom Web-Interface angezeigte Liste der Gruppenmitglieder (die Seite **Mitglieder**) ermöglicht die Unterscheidung zwischen normalen Gruppenmitgliedern und temporären Gruppenmitgliedern. Es ist auch möglich, die temporären Mitglieder, die laut Planung zukünftig zur Gruppe hinzugefügt werden sollen, jedoch aktuell noch keine Mitglieder der Gruppe sind, auszublenden oder anzuzeigen.
- **Temporäre Mitgliedschaft eines Objekts anzeigen** Die Liste der Gruppenmitgliedschaften für ein bestimmtes Objekt (die Seite **Mitglied von**) ermöglicht die Unterscheidung zwischen den Gruppen, in denen das Objekt ein normales Mitglied ist, und den Gruppen, in denen das Objekt ein temporäres Mitglied ist. Es ist auch möglich, die Gruppen auszublenden oder anzuzeigen, in die das Objekt laut Planung zukünftig hinzugefügt werden soll.

- **Temporäre Gruppenmitgliedschaften neu planen** Sowohl die Seite **Mitglieder** als auch die Seite **Mitglied von** bieten die Möglichkeit, die Einstellungen für die temporäre Gruppenmitgliedschaft anzuzeigen oder zu ändern. Auf der Seite **Mitglieder** für eine bestimmte Gruppe können Sie ein Mitglied auswählen und das Datum und die Uhrzeit, wann das Mitglied zur Gruppe hinzugefügt bzw. aus ihr entfernt werden soll, anzeigen oder ändern. Auf der Seite **Mitglied von** für ein bestimmtes Objekt können Sie eine Gruppe auswählen und das Datum und die Uhrzeit, wann das Objekt zur Gruppe hinzugefügt bzw. aus ihr entfernt werden soll, anzeigen oder ändern.
- **Temporäres Mitglied zu permanentem Mitglied machen** Die Einstellungen für die temporäre Gruppenmitgliedschaft bieten die Möglichkeit, anzugeben, dass das Objekt nicht aus der Gruppe entfernt werden soll und somit ein temporäres Mitglied zu einem permanenten Mitglied zu machen. Wenn die Einstellungen für die temporäre Gruppenmitgliedschaft für ein bestimmtes Objekt so konfiguriert sind, dass ein Objekt sofort zu einer bestimmten Gruppe hinzugefügt und nie aus der Gruppe entfernt wird, dann wird das Objekt zu einem normalen Mitglied dieser Gruppe. Entsprechend wird ein normales Mitglied, wenn andere Einstellungen für die temporäre Gruppenmitgliedschaft angegeben werden, in ein temporäres Mitglied konvertiert.
- **Temporäre Gruppenmitglieder entfernen** Sowohl die Seite **Mitglieder** als auch die Seite **Mitglied von** bietet die Funktion zum Entfernen von Gruppenmitgliedschaften (temporär oder normal). Wenn Sie die Funktion „Entfernen" auf temporäre Mitglieder einer Gruppe anwenden, dann werden die Mitglieder zusammen mit allen Einstellungen für die temporäre Gruppenmitgliedschaft, die für diese Mitglieder gelten, entfernt. Gleiches gilt, wenn Sie die Funktion „Entfernen" auf Gruppen anwenden, in denen ein bestimmtes Objekt ein temporäres Mitglied ist.

Mit der Funktion der temporären Gruppenmitgliedschaft gewährleistet ActiveRoles Server, dass Benutzer nur so lange Mitglieder in Gruppen sind, wie dies erforderlich ist. Die temporäre Gruppenmitgliedschaft wird dann erzwungen, wenn diese benötigt wird, und die Gefahr, Gruppenmitgliedschaften länger als erforderlich aufrecht zu erhalten, wird somit vermieden.

Verwenden von temporären Gruppenmitgliedschaften

Durch die Verwendung von temporären Gruppenmitgliedschaften können Sie Gruppenmitgliedschaften von Objekten wie etwa Benutzer- oder Computerkonten verwalten, die nur für einen bestimmten Zeitraum Mitglieder von bestimmten Gruppen sein müssen. Diese Funktion von ActiveRoles Server bietet Ihnen Flexibilität hinsichtlich der Entscheidung, welche Objekte wie lange Gruppenmitgliedschaften erfordern. Außerdem ermöglicht sie eine einfache Verfolgung dieser Objekte.

Dieser Abschnitt beschreibt die Aufgaben im Zusammenhang mit der Verwaltung von temporären Gruppenmitgliedschaften in der ActiveRoles Server-Konsole. Wenn Sie zur Anzeige und Änderung von Gruppenmitgliedschaftslisten berechtigt sind, dann können Sie temporäre Gruppenmitglieder hinzufügen, anzeigen und entfernen sowie Einstellungen für die temporäre Gruppenmitgliedschaft von Gruppenmitgliedern anzeigen und bearbeiten.

Hinzufügen von temporären Mitgliedern

Ein temporäres Mitglied einer Gruppe ist ein Objekt wie etwa ein Benutzer, ein Computer oder eine Gruppe, das für das Hinzufügen zur Gruppe bzw. zum Löschen aus der Gruppe geplant ist. Sie können temporäre Mitglieder mit Hilfe der ActiveRoles Server-Konsole hinzufügen und konfigurieren.

Gehen Sie folgendermaßen vor, um temporäre Mitglieder zu einer Gruppe hinzuzufügen:

1. Klicken Sie in der ActiveRoles Server-Konsole mit der rechten Maustaste auf die Gruppe und klicken Sie dann auf **Eigenschaften**.
2. Klicken Sie auf der Registerkarte **Mitglieder** im Dialogfeld **Eigenschaften** auf **Hinzufügen**.
3. Klicken Sie im Dialogfeld **Objekte auswählen** auf **Einstellungen für die temporäre Gruppenmitgliedschaft**.
4. Wählen Sie im Dialogfeld **Einstellungen für die temporäre Gruppenmitgliedschaft** die entsprechenden Optionen und klicken Sie dann auf **OK**:
   - Um die temporären Mitglieder an einem bestimmten Datum in der Zukunft zur Gruppe hinzuzufügen, wählen Sie **An diesem Datum** unter **Zur Gruppe hinzufügen** und anschließend das gewünschte Datum und die gewünschte Uhrzeit aus.
   - Um die temporären Mitglieder sofort zur Gruppe hinzuzufügen, wählen Sie **Jetzt** unter **Zur Gruppe hinzufügen**.
   - Um die temporären Mitglieder an einem bestimmten Datum aus der Gruppe zu entfernen, wählen Sie **An diesem Datum** unter **Aus der Gruppe entfernen** und anschließend das gewünschte Datum und die gewünschte Uhrzeit aus.
   - Um die temporären Mitglieder auf unbestimmte Zeit in der Gruppe zu behalten, wählen Sie **Nie** unter **Aus der Gruppe entfernen**.
5. Geben Sie im Dialogfeld **Objekte auswählen** die Namen der Objekte ein, die Sie zu temporären Mitgliedern der Gruppe machen möchten, oder wählen Sie sie aus und klicken Sie dann auf **OK**.

6. Klicken Sie auf **Anwenden** im Dialogfeld **Eigenschaften** für die Gruppe.

- Um temporäre Mitglieder einer Gruppe hinzuzufügen, müssen Sie befugt sein, Mitglieder zur Gruppe hinzuzufügen bzw. aus ihr zu entfernen. Die entsprechende Befugnis kann durch Anwenden der Zugriffsvorlage **Groups – Add/Remove Members** delegiert werden.
- Sie können ein Objekt zu einem temporären Mitglied von bestimmten Gruppen machen, indem Sie die Objekteigenschaften anstelle der Gruppeneigenschaften verwalten. Öffnen Sie das Dialogfeld **Eigenschaften** für dieses Objekt und klicken Sie dann auf der Registerkarte **Mitglied von** auf **Hinzufügen**. Geben Sie im Dialogfeld **Objekte auswählen** die Einstellungen für die temporäre Gruppenmitgliedschaft an und geben Sie dann die Namen der Gruppen abhängig von Ihrer Situation an.

Anzeigen von temporären Mitgliedern

Die von der ActiveRoles Server-Konsole angezeigte Liste der Gruppenmitglieder ermöglicht die Unterscheidung zwischen normalen Gruppenmitgliedern und temporären Gruppenmitgliedern. Es ist auch möglich, so genannte *ausstehende Mitglieder* auszublenden oder anzuzeigen. Dies sind die temporären Mitglieder, die laut Planung zukünftig zur Gruppe hinzugefügt werden sollen, jedoch aktuell noch keine Mitglieder der Gruppe sind.

So zeigen Sie temporäre Mitglieder einer Gruppe an:

1. Klicken Sie in der ActiveRoles Server-Konsole mit der rechten Maustaste auf die Gruppe und klicken Sie dann auf **Eigenschaften**.
2. Untersuchen Sie die Liste auf der Registerkarte **Mitglieder** im Dialogfeld **Eigenschaften**:
   - Ein kleines Uhrsymbol wird über dem Symbol für die temporären Mitglieder angezeigt.
   - Wenn das Kontrollkästchen **Ausstehende Mitglieder anzeigen** aktiviert ist, enthält die Liste auch die temporären Mitglieder, die noch nicht zur Liste hinzugefügt wurden. Symbole, die solche Mitglieder angeben, werden orange angezeigt.

Die Liste der Gruppenmitgliedschaften für ein bestimmtes Objekt ermöglicht die Unterscheidung zwischen den Gruppen, in denen das Objekt ein normales Mitglied ist, und den Gruppen, in denen das Objekt ein temporäres Mitglied ist. Es ist auch möglich, so genannte *ausstehende Gruppenmitgliedschaften* auszublenden oder anzuzeigen. Ausstehende Gruppenmitgliedschaften sind die Gruppen, in die das Objekt laut Planung zukünftig hinzugefügt werden soll.

So zeigen Sie die Gruppen an, in denen ein Objekt ein temporäres Mitglied ist:

1. Klicken Sie in der ActiveRoles Server-Konsole mit der rechten Maustaste auf das Objekt und klicken Sie dann auf **Eigenschaften**.
2. Untersuchen Sie die Liste auf der Registerkarte **Mitglied von** im Dialogfeld **Eigenschaften**:
   - Ein kleines Uhrsymbol wird über dem Symbol für die Gruppen angezeigt, in denen das Objekt ein temporäres Mitglied ist.
   - Wenn das Kontrollkästchen **Ausstehende Gruppenmitglieder anzeigen** aktiviert ist, enthält die Liste auch die Gruppen, zu denen das Objekt laut Planung zukünftig hinzugefügt werden soll. Symbole, die solche Gruppen angeben, werden orange angezeigt.

Neuplanen von temporären Gruppenmitgliedschaften

Die Einstellungen für die temporäre Gruppenmitgliedschaft für ein Gruppenmitglied umfassen die Einstellungen *Startzeit* und *Endzeit*.

Die Startzeit gibt an, wann das Objekt zur Gruppe hinzugefügt wird. Hierbei kann es sich um ein bestimmtes Datum und eine bestimmte Uhrzeit oder um eine Angabe, dass das Objekt sofort zur Gruppe hinzugefügt werden soll, handeln.

Die Endzeit gibt an, wann das Objekt aus der Gruppe entfernt werden soll. Hierbei kann es sich um ein bestimmtes Datum und eine bestimmte Uhrzeit oder um eine Angabe, dass das Objekt nicht aus der Gruppe entfernt werden soll, handeln.

Sie können sowohl die Startzeit- als auch die Endzeiteinstellungen mit Hilfe der ActiveRoles Server-Konsole anzeigen und ändern.

Gehen Sie folgendermaßen vor, um die Start- oder Endzeit für ein Mitglied einer Gruppe anzuzeigen oder zu ändern:

1. Klicken Sie in der ActiveRoles Server-Konsole mit der rechten Maustaste auf die Gruppe und klicken Sie dann auf **Eigenschaften**.
2. Klicken Sie in der Liste auf der Registerkarte **Mitglieder** im Dialogfeld **Eigenschaften** auf das Mitglied und klicken Sie dann auf die Schaltfläche **Einstellungen für die temporäre Gruppenmitgliedschaft**.
3. Verwenden Sie das Dialogfeld **Einstellungen für die temporäre Gruppenmitgliedschaft**, um die Start- oder Endzeit anzuzeigen oder zu ändern.

Das Dialogfeld **Einstellungen für die temporäre Gruppenmitgliedschaft** umfasst die folgenden Optionen:

- **Zur Gruppe hinzufügen | Jetzt** Gibt an, dass das Objekt sofort zur Gruppe hinzugefügt werden soll.
- **Zur Gruppe hinzufügen | An diesem Datum** Gibt das Datum und die Uhrzeit an, an dem bzw. zu der das Objekt zur Gruppe hinzugefügt werden soll.
- **Aus der Gruppe entfernen | Nie** Gibt an, dass das Objekt nicht aus der Gruppe entfernt werden soll.
- **Aus der Gruppe entfernen | An diesem Datum** Gibt das Datum und die Uhrzeit an, an dem bzw. zu der das Objekt aus der Gruppe entfernt werden soll.

Für normale Mitglieder sind die Optionen **Zur Gruppe hinzufügen** und **Aus Gruppe entfernen** auf **Bereits hinzugefügt** bzw. **Nie** gesetzt. Sie können ein bestimmtes Datum für jede dieser Optionen festlegen, um ein normales Mitglied in ein temporäres Mitglied umzuwandeln.

- Sie können die Start- und Endzeiteinstellungen anzeigen und ändern, indem Sie ein Objekt anstelle der Gruppen, in denen das Objekt Mitglied ist, verwalten. Öffnen Sie das Dialogfeld **Eigenschaften** für dieses Objekt und wählen Sie dann auf der Registerkarte **Mitglied von** die Gruppe aus, für die Sie die Start- oder Endzeiteinstellungen des Objekts verwalten möchten, und klicken Sie dann auf **Einstellungen für die temporäre Gruppenmitgliedschaft**.
- Auf der Registerkarte **Mitglieder** oder **Mitglied von** können Sie die Start- oder Endzeiteinstellungen für mehrere Mitglieder oder Gruppen gleichzeitig ändern. Wählen Sie in der Liste auf der Registerkarte zwei oder mehr Elemente aus und klicken Sie dann auf **Einstellungen für die temporäre Gruppenmitgliedschaft**. Aktivieren Sie dann im Dialogfeld **Einstellungen für die temporäre Gruppenmitgliedschaft** die entsprechenden Kontrollkästchen, um die zu ändernden Einstellungen anzugeben, und nehmen Sie dann die gewünschten Änderungen vor.

Entfernen von temporären Mitgliedern

Sie können temporäre Gruppenmitglieder auf die gleiche Weise entfernen wie normale Gruppenmitglieder. Durch das Entfernen eines temporären Mitglieds aus einer Gruppe werden die Einstellungen für die temporäre Gruppenmitgliedschaft für dieses Objekt in Hinblick auf diese Gruppe gelöscht. Folglich wird das Objekt nicht zur Gruppe hinzugefügt. Wenn das Objekt zum Zeitpunkt des Entfernens bereits zu der Gruppe gehört, dann wird es aus der Gruppe entfernt.

Gehen Sie folgendermaßen vor, um ein temporäres Mitglied aus einer Gruppe zu entfernen:

1. Klicken Sie in der ActiveRoles Server-Konsole mit der rechten Maustaste auf die Gruppe und klicken Sie dann auf **Eigenschaften**.
2. Klicken Sie auf der Registerkarte **Mitglieder** im Dialogfeld **Eigenschaften** auf das Mitglied, klicken Sie dann auf **Entfernen** und klicken Sie anschließend auf **Anwenden**.

Sie können ein Objekt, das ein temporäres Mitglied einer Gruppe ist, entfernen, indem Sie das Objekt anstelle der Gruppe verwalten. Öffnen Sie das Dialogfeld **Eigenschaften** für dieses Objekt und wählen Sie dann auf der Registerkarte **Mitglied von** die Gruppe aus der Liste aus und klicken Sie dann auf **Entfernen**.

9

Gruppenfamilie

- Grundlegendes zu Gruppenfamilien
- Erstellen einer Gruppenfamilie
- Verwalten einer Gruppenfamilie
- Szenario: Abteilungsbezogene Gruppenfamilie

Grundlegendes zu Gruppenfamilien

ActiveRoles Server stellt eine separate Kategorie regelorientierter Richtlinien speziell für die automatische Gruppenbereitstellung (AutoProvisioning für Gruppen) bereit. Jede Richtlinie dieser Kategorie, die als *Gruppenfamilie* bezeichnet wird, dient als Kontrollmechanismus für die Erstellung und Auffüllung von Gruppen.

Die Gruppenfamilie erstellt automatisch Gruppen und pflegt Gruppenmitgliedschaftslisten. Dabei hält sie konfigurierbare Regeln ein. Die Gruppenmitgliedschaft kann somit anhand von Objekteigenschaften im Verzeichnis definiert werden. Die Gruppenfamilie ermöglicht außerdem das Erstellen neuer Gruppen anhand neuer Werte, die in Objekteigenschaften erkannt werden.

Wenn Sie beispielsweise Gruppen anhand des geografischen Standorts verwalten möchten, können Sie eine Gruppenfamilie konfigurieren, die Gruppen für jeden Wert in der Eigenschaft „Stadt" von Benutzerkonten erstellt und pflegt. Die Gruppenfamilie erkennt alle Werte dieser Eigenschaft im Verzeichnis und generiert für jeden Wert eine Gruppe. Diese wird mit den Benutzern aufgefüllt, die denselben Wert für die Eigenschaft „Stadt" aufweisen. Wenn der Eigenschaft „Stadt" für einige Benutzer ein neuer Wert zugewiesen wird, erstellt die Gruppenfamilie automatisch eine neue Gruppe für diese Benutzer. Wenn für einen Benutzer der Wert der Eigenschaft „Stadt" geändert wird, ändert die Gruppenfamilie die Gruppenmitgliedschaft für diesen Benutzer entsprechend.

Die Konfiguration einer Gruppenfamilie muss nicht auf eine einzelne Objekteigenschaft beschränkt sein. Sie kann aus so vielen Eigenschaften kombiniert werden wie nötig. Beispielsweise kann eine Gruppenfamilie so eingerichtet werden, dass sie die Eigenschaften für die Abteilung und die Stadt berücksichtigt. Folglich erstellt und pflegt die Gruppenfamilie eine separate Gruppe für jede Abteilung an jedem geografischen Standort.

Entwurfsübersicht

Die wichtigsten Entwurfselemente der Gruppenfamilie sind Folgende:

- **Bereichsdefinierung nach Objektspeicherort** Bestimmt die Verzeichniscontainer, die die von der Gruppenfamilie zu verwaltenden Objekte enthalten. Der Bereich der Gruppenfamilie kann auf bestimmte Container eingeschränkt werden, sodass sie sich nur auf die Objekte in diesen Containern auswirkt.
- **Bereichsdefinierung nach Objekttyp und Eigenschaft** Bestimmt den Typ der Objekte, z.B. Benutzer oder Computer, die von der Gruppenfamilie verwaltet werden sollen. Der Bereich der Gruppenfamilie kann so auf eine Gruppe von Objekten eines bestimmten Typs beschränkt werden. Um den Bereich weiter zu verfeinern, können Sie einen Filter anwenden, mit dem die Gruppenfamilie nur die Objekte verwaltet, die bestimmte Bedingungen in Bezug auf Eigenschaften erfüllen.
- **Gruppierung nach Objekteigenschaft** Die Gruppenfamilie teilt die verwalteten Objekte (den Bereich) in *Gruppierungen* ein. Jede Gruppierung besteht aus den Objekten, bei denen die angegebenen Eigenschaften (die so genannten *Gruppieren-nach-Eigenschaften*) die gleiche Kombination von Werten aufweisen. Wenn beispielsweise die Abteilungseigenschaft als Gruppieren-nach-Eigenschaft für Benutzerobjekte angegeben ist, enthält jede Gruppierung nur die Benutzer aus einer bestimmten Abteilung.

- **Erstellen oder Erfassung von Gruppen** Normalerweise erstellt die Gruppenfamilie für jede Gruppierung eine neue Gruppe, um sie der Gruppierung zuzuordnen (mit ihr zu verknüpfen). Dabei wird sichergestellt, dass nur Mitglieder dieser Gruppierung in der Gruppe enthalten sind. Beim Erstellen von Gruppen für Gruppierungen verwendet die Gruppenfamilie Gruppenbenennungsregeln, die auf den Werten der Gruppieren-nach-Eigenschaften basieren. Eine weitere Option ist die manuelle Verknüpfung vorhandener Gruppen mit Gruppierungen; dieser Vorgang wird als *Erfassen von Gruppen* bezeichnet.
- **Pflege von Gruppenmitgliedschaftsliste auf der Grundlage von Gruppierungen** Während jeder folgenden Ausführung der Gruppenfamilie werden die Gruppierungen neu berechnet, und die zugehörigen Gruppen werden anhand der Änderungen in den Gruppierungen aktualisiert. Mit diesem Vorgang wird sichergestellt, das die Gruppe, die der jeweiligen Gruppierung zugeordnet ist, genau dieselben Objekte enthält wie die Gruppierung. Wenn eine neue Gruppierung gefunden wird, erstellt die Gruppenfamilie eine Gruppe, verknüpft die Gruppe mit der neuen Gruppierung, und füllt die Mitgliedschaftsliste der Gruppe mit den Objekten dieser Gruppierung auf.
- **Anpassen der Eigenschaften von generierten Gruppen** Wenn die Gruppenfamilie eine neue Gruppe für eine Gruppierung erstellt, werden der Name und andere Eigenschaften der neuen Gruppe anhand der Regeln angepasst, die in der Gruppenfamilienkonfiguration definiert sind. Mit diesen Regeln wird außerdem Folgendes bestimmt: der Container, in dem neue Gruppen erstellt werden sollen, die Einstellungen für Gruppentyp und Bereich sowie Einstellungen im Zusammenhang mit Exchange, z.B. die Frage, ob die generierten Gruppen E-Mail-fähig sein sollen.
- **Ausführen auf einer geplanten Basis** Die Gruppenfamilie ist eine zustandsbasierte Richtlinie. Bei jeder Ausführung analysiert sie den Zustand der Verzeichnisdaten und führt anhand der Analyseergebnisse bestimmte Bereitstellungsaktionen aus. Die Gruppenfamilie kann für die Ausführung in regelmäßigen Intervallen geplant werden. Dabei wird sichergestellt, dass alle notwendigen Gruppen vorhanden sind und dass die Gruppenmitgliedschaftslisten aktuell und richtig sind. Außerdem kann die Gruppenfamilie jederzeit manuell ausgeführt werden.
- **Vorgangsübersicht-Protokoll** ActiveRoles Server stellt ein Protokoll mit Zusammenfassungsinformationen zur letzten Ausführung der Gruppenfamilie bereit. Das Protokoll enthält ggf. Beschreibungen der Fehlersituationen, die während der Ausführung aufgetreten sind, und fasst die quantitativen Ergebnisse der Ausführung zusammen, z.B. die Anzahl aktualisierter Gruppen, die Anzahl erstellter Gruppen und die Anzahl der Objekte, deren Gruppenmitgliedschaften geändert wurden.

Funktionsweise

Die Gruppenfamilienkonfiguration gibt Regeln an, mit denen Folgendes bestimmt wird:

- **Bereich** Die von der Gruppenfamilie verwalteten Verzeichnisobjekte werden als der *Bereich* bezeichnet. Der Bereich kann auf Objekte einer bestimmten Kategorie (wie z.B. Benutzerobjekte) eingeschränkt werden, die sich in bestimmten Organisationseinheiten befinden. Außerdem kann der Bereich durch Filterung weiter verfeinert werden.
- **Gruppierungen** Die Gruppenfamilie teilt den Bereich in Teilmengen auf, die als *Gruppierungen* bezeichnet werden. Jede Gruppierung besteht aus Objekten, die für bestimmte Eigenschaften die gleichen Werte aufweisen. Diese Eigenschaften werden als *Gruppieren-nach-Eigenschaften* bezeichnet. Eine Gruppierung wir also durch eine bestimmte Kombination von Werten der Gruppieren-nach-Eigenschaften identifiziert. Die Liste aller dieser Kombinationen wird als Teil der Gruppenfamilienkonfiguration gespeichert und gepflegt.

- **Gruppennamen** Falls nichts anderes angegeben ist, erstellt die Gruppenfamilie für jede gefundene neue Gruppierung eine neue Gruppe. Der Gruppenname wird anhand der Benennungsregeln für Gruppen generiert. Sie können auch vorhandene Gruppen manuell zu einigen Gruppierungen zuweisen. Dann *erfasst* die Gruppenfamilie diese Gruppen.
- **Verknüpfungen** Für jede Gruppierung erstellt oder erfasst die Gruppenfamilie eine Gruppe, verknüpft sie mit der Gruppierung und füllt sie mit den Objekten der Gruppierung auf. Während jeder folgenden Ausführung verwendet die Gruppenfamilie die Verknüpfungsinformationen, um die Gruppe zu erkennen, die mit der Gruppierung verknüpft ist, und aktualisiert die Mitgliedschaftsliste dieser Gruppe anhand der Änderungen in der Gruppierung. Die Gruppen, deren Informationen der Gruppenfamilie über die Verknüpfungen zur Verfügung stehen, werden als *kontrollierte Gruppen* bezeichnet.

Während der ersten Ausführung führt die Gruppenfamilie also Folgendes aus:

1. Der Bereich wird berechnet und analysiert, um eine Liste aller vorhandenen Wertekombinationen der Gruppieren-nach-Eigenschaften zu erstellen. Die Liste wird dann der Gruppenfamilienkonfiguration hinzugefügt.
2. Für jede Kombination von Werten wird eine Gruppierung berechnet, die aus allen Objekten im Bereich besteht, deren Gruppieren-nach-Eigenschaften auf die aus dieser Kombination abgeleiteten Werte festgelegt sind.
3. Für jede Gruppierung wird eine Gruppe erstellt oder erfasst und mit der Gruppierung verknüpft. Die Gruppenfamilienkonfiguration wird mit Informationen zu diesen Verknüpfungen aktualisiert. Die Gruppenfamilienkonfiguration bestimmt, ob eine Gruppe erstellt oder erfasst werden soll.
4. Für jede Gruppe, die mit einer bestimmten Gruppierung (kontrollierten Gruppe) verknüpft ist, wird die Mitgliedschaftsliste so aktualisiert, dass sie nur die Objekte dieser Gruppierung enthält. Alle vorhandenen Mitglieder werden aus der Gruppe entfernt. Dann werden alle in der Gruppierung gefundenen Objekte der Gruppe hinzugefügt.

Während einer weiteren Ausführung führt die Gruppenfamilie Folgendes aus:

1. Der Bereich wird berechnet und analysiert, um eine Liste aller vorhandenen Wertekombinationen der Gruppieren-nach-Eigenschaften zu erstellen. Die Gruppenfamilienkonfiguration wird dann anhand dieser Liste aktualisiert.
2. Für jede Kombination von Werten wird eine Gruppierung berechnet, die aus allen Objekten im Bereich besteht, deren Gruppieren-nach-Eigenschaften auf die aus dieser Kombination abgeleiteten Werte festgelegt sind.
3. Für jede Gruppierung wird eine Suche ausgeführt, die auf Verknüpfungsinformationen basiert, um die mit dieser Gruppierung verknüpfte Gruppe zu erkennen. Wenn die Gruppe gefunden wurde, wird ihre Mitgliedschaftsliste so aktualisiert, dass die Gruppe nur die in der Gruppierung gefundenen Objekte enthält. Andernfalls wird eine Gruppe erstellt oder erfasst, mit der Gruppierung verknüpft und mit den in der Gruppierung gefundenen Objekten aufgefüllt.

Beim Erstellen einer Gruppe für eine bestimmte Gruppierung generiert die Gruppenfamilie den Gruppennamen anhand der Benennungsregeln für Gruppen. Die Regeln definieren einen Namen, der auf der Wertekombination der Gruppieren-nach-Eigenschaften basiert, die die Gruppierung identifiziert. Die Benennungsregeln für Gruppen sind Teil der Gruppenfamilienkonfiguration.

Bei der Erfassung einer vorhandenen Gruppe für eine bestimmte Gruppierung verwendet die Gruppenfamilie eine Verknüpfung zwischen Gruppe und Gruppierung, die manuell erstellt und als Teil der Gruppenfamilienkonfiguration gespeichert wird. Die Verknüpfung gibt die Wertekombination der Gruppieren-nach-Eigenschaften an, um die Gruppierung zu identifizieren, und bestimmt die Gruppe, die mit dieser Gruppierung verknüpft werden soll.

Beim Füllen einer Gruppe verarbeitet die Gruppenfamilie nur die Objekte, die aus derselben Active Directory-Domäne wie die Gruppe selbst stammen. Wenn sich ein bestimmtes Objekt (wie etwa ein Benutzerkonto) in einer anderen Domäne befindet, kann die Gruppenfamilie das Objekt selbst dann nicht zur Gruppe hinzufügen, wenn dies von der Gruppenfamilie gemäß ihrer Konfiguration erwartet wird. Diese Einschränkung ist Absicht.

Erstellen einer Gruppenfamilie

Die Erstellung einer Gruppenfamilie besteht aus den folgenden zwei Schritten:

1. Erstellen der Gruppenfamilienkonfiguration
2. Ausführen der Gruppenfamilie zur Erstellung oder Erfassung von Gruppen

Die ActiveRoles Server-Konsole enthält den Assistenten „Neue Gruppenfamilie", mit dem Sie die Gruppenfamilienkonfiguration erstellen können. Der Assistent erstellt eine Gruppe, die als *Konfigurationsspeichergruppe* bezeichnet wird, und füllt sie mit den von Ihnen angegebenen Konfigurationsdaten auf.

Sie können beliebig viele Gruppenfamilien erstellen. Dabei steuert jede Gruppenfamilie eine bestimmte Sammlung von Gruppen. Wenn Sie eine Gruppe mit einer Gruppierung verknüpfen, stellt das Gruppenfamilienmodul sicher, dass die Gruppe nur von der Gruppenfamilie kontrolliert wird, die die Verknüpfung erstellt hat. So werden Konflikte vermieden.

Schrittweise Anleitungen bezüglich der Erstellung und Verwaltung einer Gruppenfamilie finden Sie in den Themen, die unter der Überschrift **Anleitungen/Verwalten von Gruppenfamilien** in der ActiveRoles Server-Hilfe aufgelistet sind.

Starten des Assistent für neue Gruppenfamilie

Sie können den Assistenten „Neue Gruppenfamilie" über die ActiveRoles Server-Konsole starten. Verwenden Sie dazu den Befehl **Neu | Gruppenfamilie** für die Organisationseinheit, in die Sie die Konfigurationsspeichergruppe platzieren möchten.

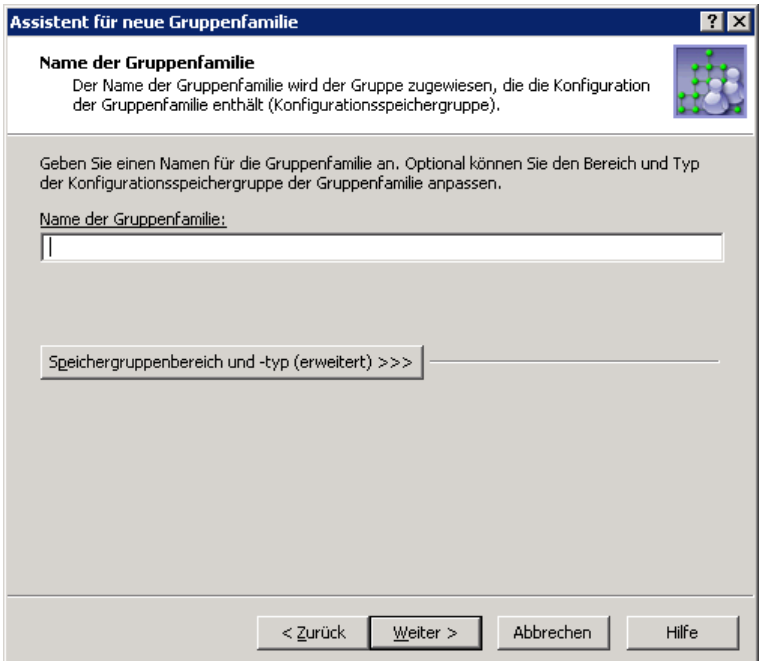
Gehen Sie folgendermaßen vor, um den Assistenten „Neue Gruppenfamilie" zu starten:

- Klicken Sie mit der rechten Maustaste auf die Organisationseinheit, die die Konfigurationsspeichergruppe der Gruppenfamilie enthalten soll, und wählen Sie **Neu | Gruppenfamilie** aus.

Name der Gruppenfamilie

Auf der ersten Seite nach der Willkommensseite stellen Sie einen Namen für die neue Gruppenfamilie bereit. Der Name wird der Gruppe zugewiesen, in der die Konfigurationsdaten der Gruppenfamilie gespeichert werden (der Konfigurationsspeichergruppe).

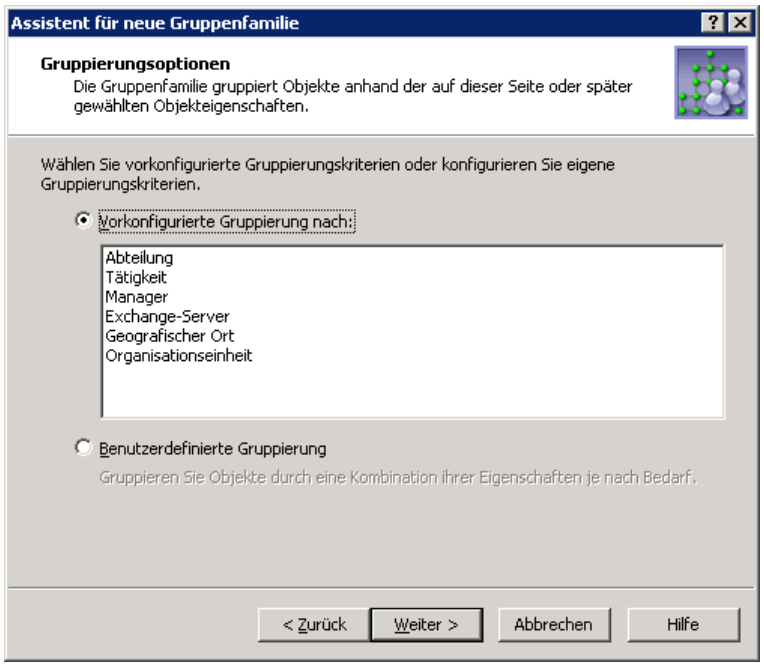
Außerdem können Sie auf dieser Seite den Typ und den Bereich der Konfigurationsspeichergruppe anpassen. Standardmäßig sind diese auf den Sicherheitstyp und den globalen Bereich festgelegt. Normalerweise müssen sie nicht geändert werden.


Assistent für neue Gruppenfamilie
Name der Gruppenfamilie
Der Name der Gruppenfamilie wird der Gruppe zugewiesen, die die Konfiguration der Gruppenfamilie enthält (Konfigurationsspeichergruppe).
Geben Sie einen Namen für die Gruppenfamilie an. Optional können Sie den Bereich und Typ der Konfigurationsspeichergruppe der Gruppenfamilie anpassen.
Name der Gruppenfamilie:
Speichergruppenbereich und -typ (erweitert) >>>
< Zurück
Weiter >
Abbrechen
Hilfe

Geben Sie einen Gruppenfamiliennamen ein und klicken Sie dann auf **Weiter**, um den Vorgang fortzusetzen.

Gruppierungsoptionen

Auf der nächsten Seite wird eine Liste häufig verwendeter Gruppierungskriterien bereitgestellt. Die Gruppenfamilie erstellt Gruppierungen anhand der Eigenschaften, die Sie auf dieser Seite auswählen können (Sie können sie aber auch später angeben).

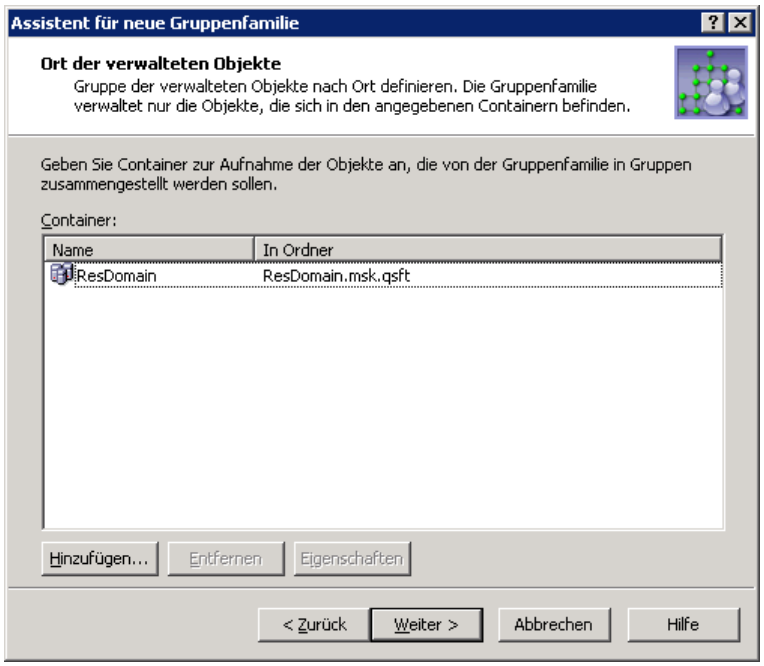


Sie können eine der folgenden Optionen auswählen:

- **Vorkonfigurierte Gruppierung** Stellt eine Liste der häufig verwendeten Gruppieren-nach-Eigenschaften bereit. Dazu gehören die Abteilung, der Titel und der geografische Standort. Wählen Sie in der Liste einen Eintrag aus, um die Gruppieren-nach-Eigenschaften anzugeben. Später können Sie auf der Seite **Gruppieren-nach-Eigenschaften** des Assistenten die Liste der ausgewählten Gruppieren-nach-Eigenschaften anzeigen oder ändern.
- **Benutzerdefinierte Gruppierung** Ermöglicht das Fortsetzen des Vorgangs ohne sofortiges Auswählen von Gruppieren-nach-Eigenschaften. Der Assistent fordert Sie später auf der Seite **Gruppieren-nach-Eigenschaften** zum Festlegen einer Liste von Gruppieren-nach-Eigenschaften auf.

Ort der verwalteten Objekte

Auf der nächsten Seite werden Sie aufgefordert, die Verzeichniscontainer anzugeben, die die von dieser Gruppenfamilie zu verwaltenden Objekte enthalten. Der Bereich der Gruppenfamilie kann auf bestimmte Container eingeschränkt werden, sodass sie sich nur auf die Objekte in diesen Containern auswirkt.


Assistent für neue Gruppenfamilie
Ort der verwalteten Objekte
Gruppe der verwalteten Objekte nach Ort definieren. Die Gruppenfamilie verwaltet nur die Objekte, die sich in den angegebenen Containern befinden.
Geben Sie Container zur Aufnahme der Objekte an, die von der Gruppenfamilie in Gruppen zusammengestellt werden sollen.
Container:
Name
In Ordner
ResDomain
ResDomain.msk.qsft
Hinzufügen...
Entfernen
Eigenschaften
< Zurück
Weiter >
Abbrechen
Hilfe

Auf dieser Seite werden die Container aufgelistet, die in den Bereich der Gruppenfamilie eingeschlossen werden sollen. Jeder Eintrag in der Liste identifiziert einen Container mit Namen und stellt den Pfad zu seinem übergeordneten Container bereit.

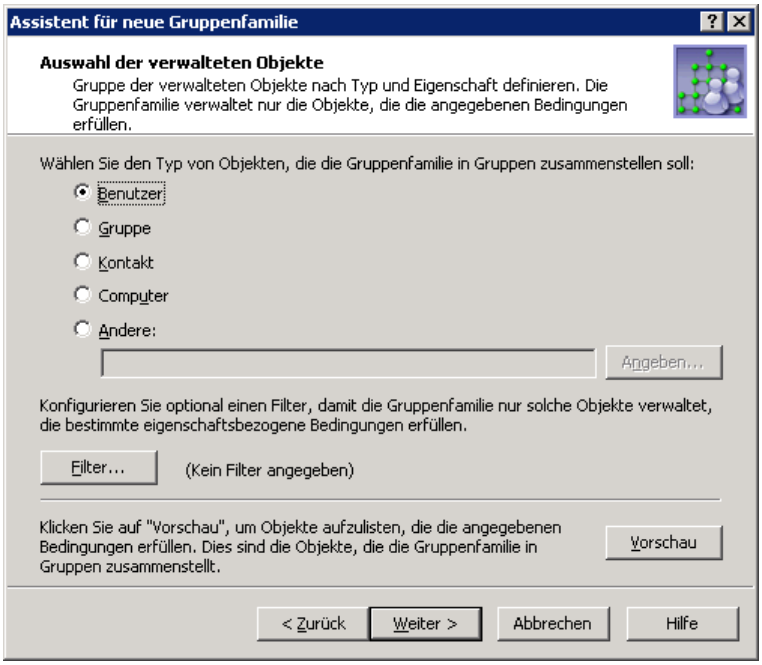
Um der Liste einen Container hinzuzufügen, klicken Sie auf **Hinzufügen** und wählen Sie den Container aus. Dann schließt der Gruppenfamilienbereich Objekte aus diesem Container ein.

Um Container aus der Liste zu entfernen, wählen Sie sie aus, und klicken Sie dann auf **Entfernen**. Dann schließt der Gruppenfamilienbereich die Objekte aus diesen Containern nicht mehr ein.

Um Eigenschaften eines Containers anzuzeigen oder zu ändern, wählen Sie ihn in der Liste aus, und klicken Sie auf **Eigenschaften**.

Auswahl der verwalteten Objekte

Auf der nächsten Seite werden Sie aufgefordert, den Typ der Objekte anzugeben, z.B. Benutzer oder Computer, die von der Gruppenfamilie verwaltet werden sollen. So wird der Bereich der Gruppenfamilie auf Objekte eines bestimmten Typs eingeschränkt. Um den Bereich weiter zu verfeinern, können Sie einen Filter anwenden, mit dem die Gruppenfamilie nur die Objekte verwaltet, die bestimmte Bedingungen in Bezug auf Eigenschaften erfüllen.


Assistent für neue Gruppenfamilie
Auswahl der verwalteten Objekte
Gruppe der verwalteten Objekte nach Typ und Eigenschaft definieren. Die Gruppenfamilie verwaltet nur die Objekte, die die angegebenen Bedingungen erfüllen.
Wählen Sie den Typ von Objekten, die die Gruppenfamilie in Gruppen zusammenstellen soll:
Benutzer
Gruppe
Kontakt
Computer
Andere:
Angeben...
Konfigurieren Sie optional einen Filter, damit die Gruppenfamilie nur solche Objekte verwaltet, die bestimmte eigenschaftsbezogene Bedingungen erfüllen.
Filter...
(Kein Filter angegeben)
Klicken Sie auf "Vorschau", um Objekte aufzulisten, die die angegebenen Bedingungen erfüllen. Dies sind die Objekte, die die Gruppenfamilie in Gruppen zusammenstellt.
Vorschau
< Zurück
Weiter >
Abbrechen
Hilfe

Sie können den Typ der Objekte auswählen, die in den Bereich der Gruppenfamilie eingeschlossen werden sollen:

- **Benutzer** Der Bereich der Gruppenfamilie schließt nur Benutzerkonten ein.
- **Gruppe** Der Bereich der Gruppenfamilie schließt nur Gruppen ein. Beachten Sie, dass die Gruppenfamilie bei dieser Option Gruppen erstellt und vorhandene Gruppen den neu erstellten Gruppen hinzufügt.
- **Kontakt** Der Bereich der Gruppenfamilie schließt nur Kontaktobjekte ein.
- **Computer** Der Bereich der Gruppenfamilie schließt nur Computerkonten ein.
- **Andere** Der Bereich der Gruppenfamilie schließt nur Verzeichnisobjekte des ausgewählten Typs ein. Klicken Sie auf **Angeben**, und wählen Sie einen Objekttyp aus.

Sie können den Gruppenfamilienbereich mit Hilfe eines Filters weiter verfeinern. Klicken Sie dazu auf **Filter**. Dann wird ein Fenster angezeigt, in dem Sie Filterkriterien anzeigen oder ändern können. Die Beschriftung neben der Schaltfläche **Filter** zeigt visuell an, ob Filterkriterien angegeben sind.

Im Fenster **Filter** können Sie eine Liste von Filterkriterien einrichten. Diese werden auch als *Bedingungen* bezeichnet. Jede Bedingung gibt eine Eigenschaft, einen Operator und einen Wert an. Je nach dem aktuellen Wert der Eigenschaft wird sie zu TRUE oder FALSE ausgewertet. Beispielsweise wird die folgende Bedingung für alle Objekte zu TRUE ausgewertet, bei denen die Beschreibung angibt, dass es sich um einen Vollzeitmitarbeiter handelt:

EIGENSCHAFT	BEDINGUNG	WERT
Beschreibung	Beginnt mit	Vollzeitmitarbeiter

Wenn Bedingungen angegeben sind, wird ein Filter angewendet, sodass der Bereich der Gruppenfamilie nur die Objekte einschließt, für die alle Bedingungen zu TRUE ausgewertet werden.

Wenn die Liste der Bedingungen leer ist, schließt der Bereich der Gruppenfamilie alle Objekte des angegebenen Typs ein, die in den angegebenen Containern enthalten sind. Es wird also keine Filterung angewendet.

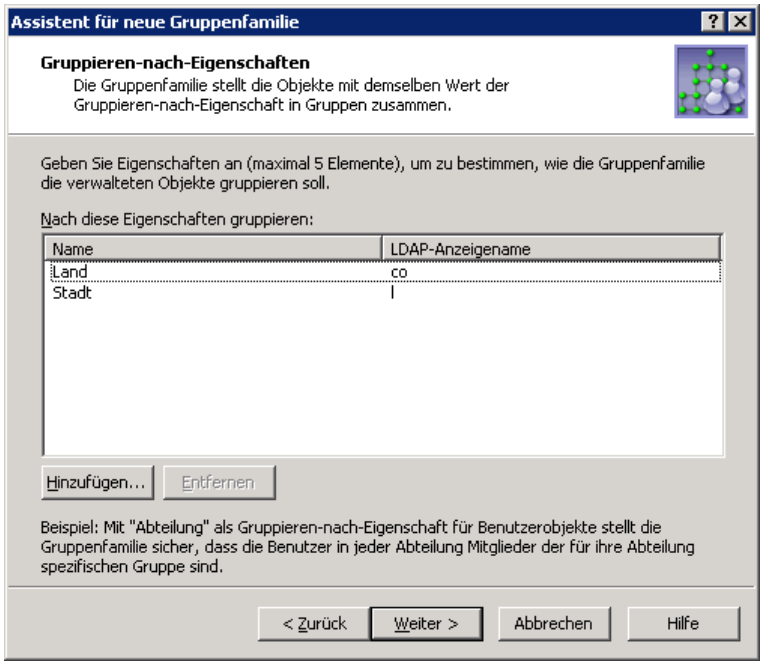
Wenn Sie einen Filter anwenden, werden nur die Objekte, die den Filterbedingungen entsprechen, zu den kontrollierten Gruppen hinzugefügt. Standardmäßig wird kein Filter angewandt, wodurch die kontrollierten Gruppen alle Objekte des angegebenen Typs enthalten. Sie können einen Standardfilter konfigurieren, indem Sie Eigenschaften auswählen und Bedingungen und Werte angeben, nach denen in den ausgewählten Eigenschaften gesucht werden soll.

Darüber hinaus haben Sie die Möglichkeit, einen erweiterten Filter zu konfigurieren, indem Sie eine entsprechende LDAP-Abfrage eingeben. Klicken Sie hierzu auf die Schaltfläche **Erweitert** im Fenster **Filter**. Beachten Sie, dass die Standard- und erweiterten Filteroptionen sich gegenseitig ausschließen. Wenn Sie einen erweiterten Filter angewandt haben, werden die Standardfiltereinstellungen ignoriert. Um zur Standardfilteroption zurückzukehren, klicken Sie auf die Schaltfläche **Standard** im Fenster „Filter". Hierdurch hat die Standardfilteroption wieder Vorrang vor der LDAP-Abfrage, auf der der erweiterte Filter basiert.

Sie können auf **Vorschau** auf der Seite **Auswahl der verwalteten Objekte** klicken, um eine Liste der Objekte anzuzeigen, die aktuell in den Gruppenfamilienbereich eingeschlossen sind. Im Fenster **Vorschau** werden die Objekte aufgelistet, die die Gruppenfamilie in Gruppen zusammenstellt.

Gruppieren-nach-Eigenschaften

Auf der nächsten Seite können Sie die Liste der Gruppieren-nach-Eigenschaften einrichten. Die Gruppenfamilie teilt die verwalteten Objekte (den Bereich) in Gruppierungen ein. Jede Gruppierung besteht aus den Objekten, bei denen die angegebenen Gruppieren-nach-Eigenschaften die gleiche Kombination von Werten aufweisen. Wenn beispielsweise die Abteilungseigenschaft als Gruppieren-nach-Eigenschaft für Benutzerobjekte angegeben ist, enthält jede Gruppierung nur die Benutzer aus einer bestimmten Abteilung. Dann stellt die Gruppenfamilie sicher, dass die Mitglieder jeder Gruppierung zu der Gruppe gehören, die mit der Gruppierung verknüpft ist.

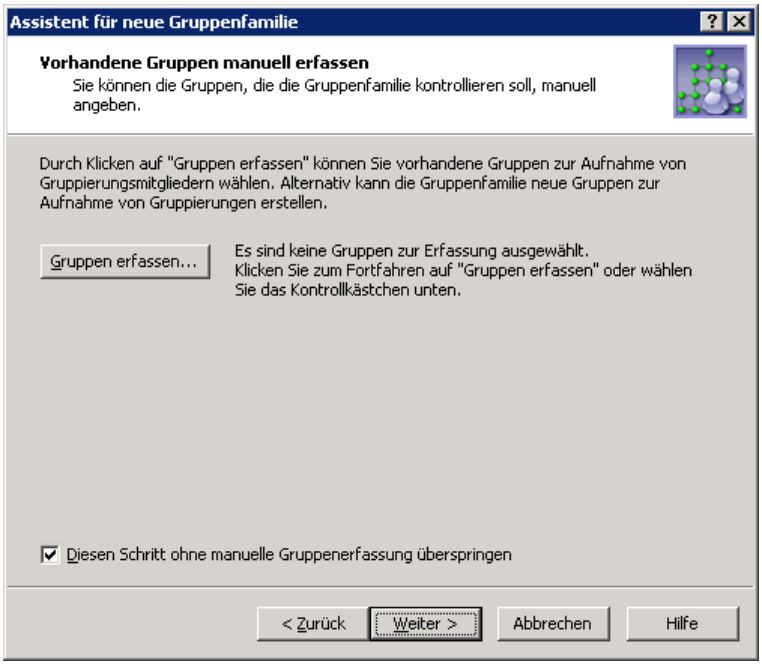

Assistent für neue Gruppenfamilie
Gruppieren-nach-Eigenschaften
Die Gruppenfamilie stellt die Objekte mit demselben Wert der Gruppieren-nach-Eigenschaft in Gruppen zusammen.
Geben Sie Eigenschaften an (maximal 5 Elemente), um zu bestimmen, wie die Gruppenfamilie die verwalteten Objekte gruppieren soll.
Nach diese Eigenschaften gruppieren:
Name
LDAP-Anzeigename
Land
co
Stadt
l
Hinzufügen...
Entfernen
Beispiel: Mit "Abteilung" als Gruppieren-nach-Eigenschaft für Benutzerobjekte stellt die Gruppenfamilie sicher, dass die Benutzer in jeder Abteilung Mitglieder der für ihre Abteilung spezifischen Gruppe sind.
< Zurück
Weiter >
Abbrechen
Hilfe

Auf der Seite werden die aktuell ausgewählten Gruppieren-nach-Eigenschaften aufgelistet. Sie können Eigenschaften der Liste hinzufügen oder aus ihr entfernen.

Die Änderungen, die Sie an der Liste auf dieser Seite vornehmen, legen die Gruppenfamilienoptionen neu fest, die von den Gruppieren-nach-Eigenschaften abhängig sind. Zu diesen Optionen gehören die Gruppenbenennungsregeln und die Liste der zu erfassenden Gruppen (wie in den folgenden beiden Abschnitten beschrieben). Wenn Sie eine Gruppieren-nach-Eigenschaft hinzufügen oder entfernen, werden die aktuellen Benennungsregeln durch die Standardbenennungsregel ersetzt, und die Liste der zu erfassenden Gruppen wird gelöscht.

Vorhandene Gruppen manuell erfassen

Auf der nächsten Seite können Sie vorhandene Gruppen mit Gruppierungen verknüpfen. Normalerweise erstellt die Gruppenfamilie automatisch eine Gruppe für jede Gruppierung und verknüpft sie mit ihr. Um dieses Verhalten für bestimmte Gruppierungen außer Kraft zu setzen, können Sie die Gruppenfamilie so konfigurieren, dass diese Gruppierungen mit den vorhandenen Gruppen verknüpft werden, die Sie angeben.


Assistent für neue Gruppenfamilie
Vorhandene Gruppen manuell erfassen
Sie können die Gruppen, die die Gruppenfamilie kontrollieren soll, manuell angeben.
Durch Klicken auf "Gruppen erfassen" können Sie vorhandene Gruppen zur Aufnahme von Gruppierungsmitgliedern wählen. Alternativ kann die Gruppenfamilie neue Gruppen zur Aufnahme von Gruppierungen erstellen.
Gruppen erfassen...
Es sind keine Gruppen zur Erfassung ausgewählt. Klicken Sie zum Fortfahren auf "Gruppen erfassen" oder wählen Sie das Kontrollkästchen unten.
Diesen Schritt ohne manuelle Gruppenerfassung überspringen
< Zurück
Weiter >
Abbrechen
Hilfe

Führen Sie auf dieser Seite eine der folgenden Aktionen aus:

- Damit die Gruppenfamilie automatisch für jede erkannte Gruppierung eine Gruppe erstellt und sie mit der Gruppierung verknüpft, aktivieren Sie das Kontrollkästchen **Diesen Schritt ohne manuelle Gruppenerfassung überspringen**.
- Um mindestens eine Verknüpfung zwischen Gruppe und Gruppierung manuell einzurichten, klicken Sie auf **Gruppen erfassen**.

Wenn Sie auf **Gruppen erfassen** klicken, wird ein Fenster angezeigt, in dem Sie eine Liste von Verknüpfungen zwischen Gruppe und Gruppierung anzeigen oder ändern können. Jeder Eintrag in der Liste schließt die folgenden Informationen ein:

- **Kombination von Werten der „Gruppieren-nach-Eigenschaften"** Die Kombination von Eigenschaftswerten, die eine Gruppierung identifiziert.
- **Gruppenname** Identifiziert die Gruppe, die mit der Gruppierung verknüpft ist.
- **In Ordner** Der kanonische Name des Containers, der die Gruppe enthält.

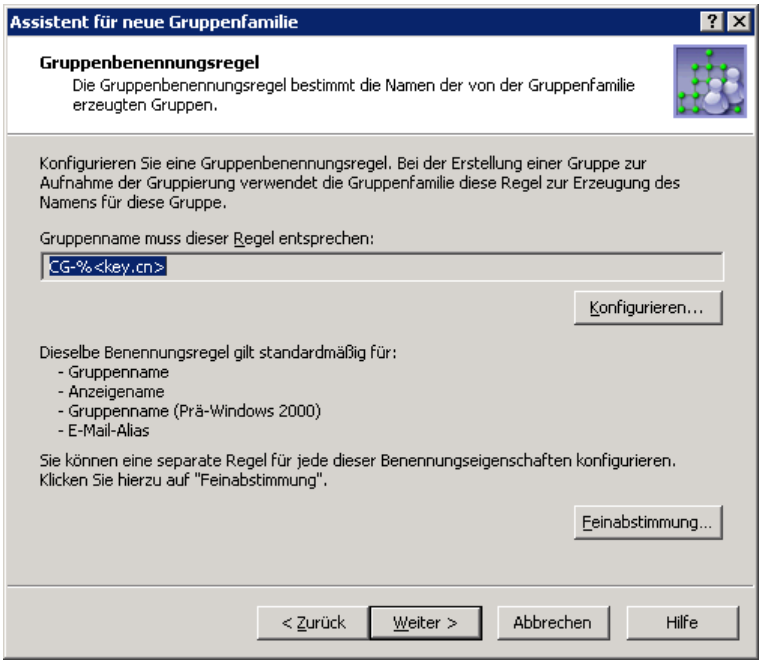
Das Fenster **Gruppen erfassen** umfasst die folgenden Schaltflächen für die Verwaltung der Liste von Verknüpfungen zwischen Gruppe und Gruppierung:

- **Hinzufügen** Öffnet ein Fenster, in dem Sie eine Gruppe auswählen und eine Gruppierung angeben können. Um eine Gruppierung anzugeben, müssen Sie einen bestimmten Wert jeder der Gruppieren-nach-Eigenschaften eingeben. Dann wird die ausgewählte Gruppe mit der Gruppierung verknüpft, die durch die eingegebene Wertekombination identifiziert wird.
- **Bearbeiten** Ermöglicht das Ändern eines Eintrags, den Sie in der Liste auswählen. Öffnet ein Fenster, in dem Sie eine andere Gruppe auswählen können oder eine andere Gruppierung angeben können, indem Sie die Wertekombination der Gruppieren-nach-Eigenschaften ändern.
- **Entfernen** Löscht die ausgewählten Verknüpfungen aus der Liste. Die Gruppenfamilie erstellt dann neue Gruppen für die Gruppierungen, die Sie aus der Liste entfernt haben.

Gruppenbenennungsregel

Auf der nächsten Seite des Assistenten können Sie die von der Gruppenfamilie verwendeten Gruppenbenennungsregeln anzeigen oder ändern.

Beim Erstellen einer neuen Gruppe generiert die Gruppenfamilie die Gruppenbenennungseigenschaften, z.B. den Gruppennamen, den Anzeigenamen, den Gruppennamen (Prä-Windows 2000) und optional den E-Mail-Alias. Falls nichts anderes angegeben ist, verwendet die Gruppenfamilie eine bestimmte Standardregel, um diese Eigenschaften anhand der Werte der Gruppieren-nach-Eigenschaften zu generieren.


Assistent für neue Gruppenfamilie
Gruppenbenennungsregel
Die Gruppenbenennungsregel bestimmt die Namen der von der Gruppenfamilie erzeugten Gruppen.
Konfigurieren Sie eine Gruppenbenennungsregel. Bei der Erstellung einer Gruppe zur Aufnahme der Gruppierung verwendet die Gruppenfamilie diese Regel zur Erzeugung des Namens für diese Gruppe.
Gruppenname muss dieser Regel entsprechen:
CG-%<key.cn>
Konfigurieren...
Dieselbe Benennungsregel gilt standardmäßig für:
- Gruppenname
- Anzeigename
- Gruppenname (Prä-Windows 2000)
- E-Mail-Alias
Sie können eine separate Regel für jede dieser Benennungseigenschaften konfigurieren. Klicken Sie hierzu auf "Feinabstimmung".
Feinabstimmung...
< Zurück
Weiter >
Abbrechen
Hilfe

Standardmäßig generiert die Gruppenfamilie die Gruppenbenennungseigenschaften anhand der folgenden Syntax: CG-%<Schlüssel.Eigenschaft1>-%<Schlüssel.Eigenschaft2>... In dieser Syntax steht CG für „Gruppieren nach Eigenschaft" dar. Beim Erstellen einer Gruppe für eine bestimmte Gruppierung setzt die Gruppenfamilie den gruppierungsspezifischen Wert der „Gruppieren-nach-Eigenschaft" in den Eintrag mit dem Namen dieser Eigenschaft ein. Beispielsweise wird in einer Gruppe, die durch den Wert **Operations (Betrieb)** der Eigenschaft **Department** identifiziert wird, der Gruppenname auf **CG-Vorgänge** festgelegt. Bei zwei „Gruppieren-nach-Eigenschaften" wie etwa **Department** und **Stadt** lautet ein Beispiel für den Gruppennamen **CG-Operations-London**.

Um die Gruppenbenennungsregel zu ändern, klicken Sie auf die Schaltfläche **Konfigurieren**. Hierdurch wird das Dialogfeld **Wert konfigurieren** geöffnet, das weiter oben in diesem Dokument beschrieben wurde (siehe „Konfigurieren einer Richtlinie für die Generierung und Validierung von Eigenschaften"). In diesem Dialogfeld können Sie einen Wert für die Bedingung **„Name" muss sein** konfigurieren, ähnlich wie beim Konfigurieren der Richtlinie „Erzeugung und Validierung von Eigenschaften".

Ein Wert entsteht durch Verkettung von mindestens einem Eintrag. Im Dialogfeld **Wert konfigurieren** befinden sich die Schaltflächen **Hinzufügen**, **Bearbeiten** und **Entfernen** für die Verwaltung der Eintragsliste. Durch Klicken auf **Hinzufügen** wird das Fenster **Eintrag hinzufügen** angezeigt.

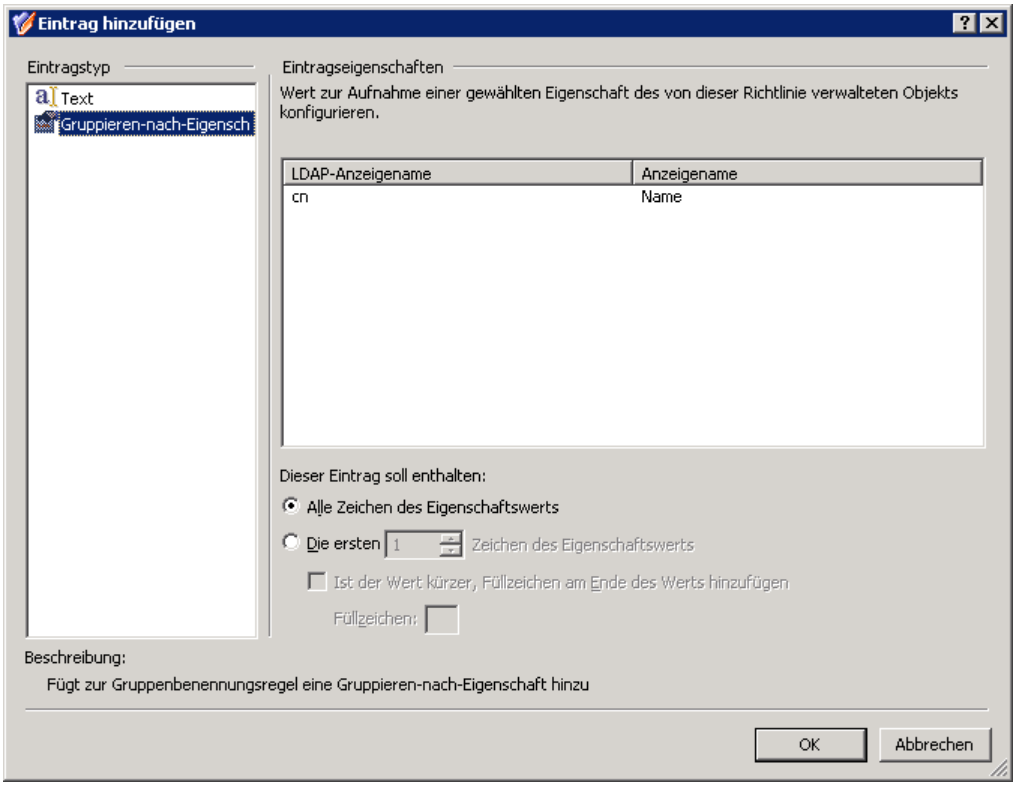
Im Fenster **Eintrag hinzufügen** können Sie den Typ des hinzuzufügenden Eintrags auswählen und den Eintrag dann konfigurieren. Folgende Eintragstypen sind verfügbar:

- **Text** Fügt der Gruppenbenennungsregel eine Textzeichenfolge hinzu.
- **Gruppieren-nach-Eigenschaft** Fügt der Gruppenbenennungsregel eine Gruppieren-nach-Eigenschaft oder einen Teil einer Gruppieren-nach-Eigenschaft hinzu.

Um eine Textzeichenfolge hinzuzufügen, geben Sie einfach im Fenster **Eintrag hinzufügen** einen Text ein. Im folgenden Unterabschnitt wird der Eintrag **Gruppieren-nach-Eigenschaft** erörtert.

Eintragstyp: Gruppieren-nach-Eigenschaft

Wenn Sie im Fenster **Eintrag hinzufügen** unter **Eintragstyp** den Typ **Gruppieren-nach-Eigenschaft** auswählen, ähnelt der Bereich **Eintragseigenschaften** der folgenden Abbildung.



Mit Hilfe des Eintragstyps **Gruppieren-nach-Eigenschaft** können Sie einen Eintrag hinzufügen, der einen Wert (oder einen Teil eines Werts) einer „Gruppieren-nach-Eigenschaft" darstellt. Wählen Sie in der Liste eine Gruppieren-nach-Eigenschaft aus, und führen Sie dann eine der folgenden Aktionen aus:

- Wenn der Eintrag den gesamten Wert der Eigenschaft enthalten soll, klicken Sie auf **Alle Zeichen des Eigenschaftswerts**.
- Wenn der Eintrag einen Teil des Eigenschaftswerts enthalten soll, klicken Sie auf **Die ersten**, und geben Sie an, wie viele Zeichen in den Eintrag eingeschlossen werden sollen.

Wenn Sie die zweite Option auswählen, können Sie das Kontrollkästchen **Ist der Wert kürzer, Füllzeichen am Ende des Werts hinzufügen** aktivieren und ein Zeichen in das Feld **Füllzeichen** eingeben. Dieses Zeichen ersetzt die fehlenden Zeichen im Wert der Eigenschaft, wenn dieser Wert kürzer ist als im Feld neben der Option **Die ersten** angegeben. Wenn Sie beispielsweise **Die ersten 12 Zeichen** angeben und **0** als Füllzeichen eingeben, wird aus dem Eigenschaftswert **Accounting (Buchhaltung)** der Eintrag **Accounting00**.

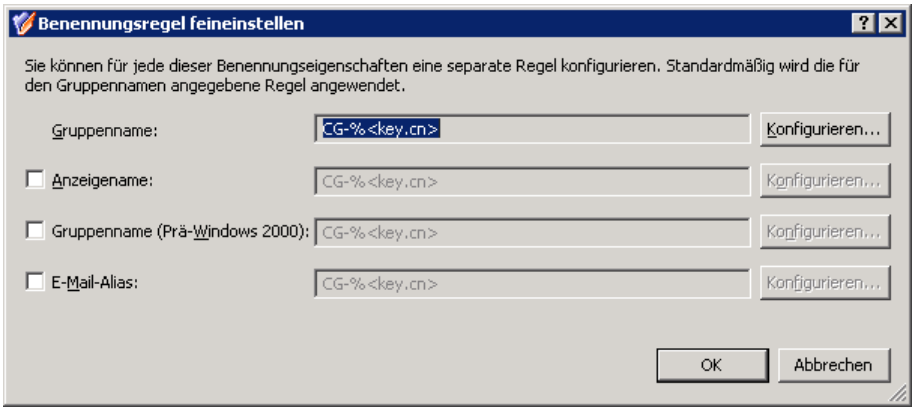
Klicken Sie nach dem Konfigurieren eines Eintrags auf **OK**, um das Fenster **Eintrag hinzufügen** zu schließen. Der Eintrag wird dem Dialogfeld **Wert konfigurieren** hinzugefügt. Klicken Sie nach dem Abschließen der Eintragsliste auf **OK**, um das Dialogfeld zu schließen. Beachten Sie, dass die Benennungsregel für jede Gruppieren-nach-Eigenschaft einen Eintrag enthalten muss.

Unterschiedliche Regeln für die Benennungseigenschaften

Standardmäßig gilt dieselbe Regel für die folgenden Benennungseigenschaften:

- Gruppenname
- Gruppenname (Prä-Windows 2000)
- Gruppenanzeigename
- E-Mail-Alias (wenn die Gruppenfamilie für die Erstellung E-Mail-fähiger Gruppen konfiguriert ist, wie weiter unten in diesem Kapitel beschrieben)

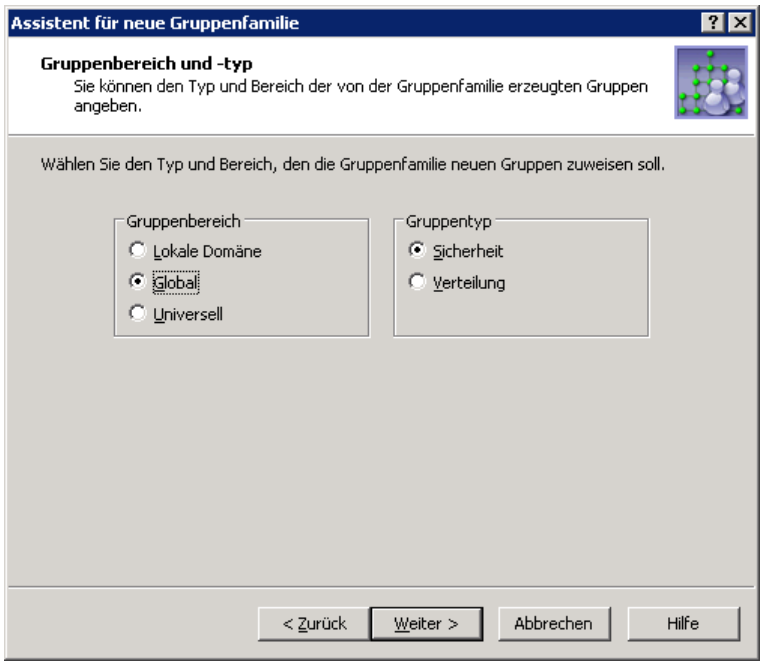
Sie können für jede dieser Benennungseigenschaften eine eigene Regel konfigurieren. Klicken Sie dazu auf der Seite **Gruppenbenennungsregel** auf **Feinabstimmung**. Dann wird ein Fenster angezeigt, in dem Sie eine Benennungseigenschaft auswählen und eine Regel für diese Eigenschaft (wie für einen Gruppennamen) konfigurieren können. Das Fenster ähnelt der folgenden Abbildung.



Möglicherweise müssen Sie für eine bestimmte Eigenschaft eine separate Regel konfigurieren und dabei Einschränkungen beachten, die für diese Eigenschaft gelten. Beispielsweise muss der Gruppenname (Prä-Windows 2000) weniger als 20 Zeichen lang sein. Um diese Anforderung zu erfüllen, aktivieren Sie das Kontrollkästchen **Gruppenname (Prä-Windows 2000)**, und klicken Sie auf **Konfigurieren**, um eine entsprechende Regel einzurichten. Wenn Sie Einträge so konfigurieren, dass sie Gruppieren-nach-Eigenschaften einschließen, begrenzen Sie die Anzahl der Zeichen in jedem Eintrag mit Hilfe der Option **Die ersten** im Fenster **Eintrag hinzufügen**.

Gruppenbereich und -typ

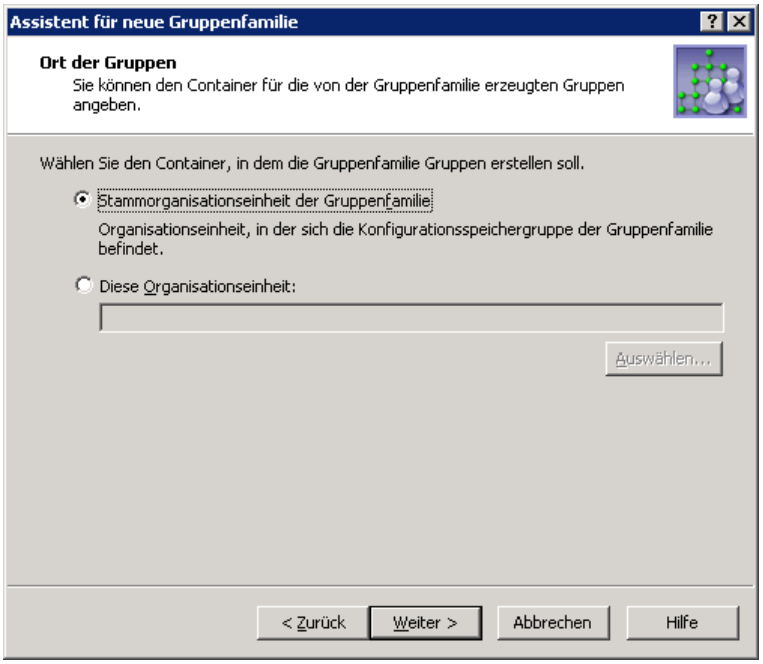
Auf der nächsten Seite können Sie den Gruppenbereich und -typ angeben, der den von der Gruppenfamilie generierten Gruppen zugewiesen werden soll.



Verfügbar sind die Standardoptionen für den Gruppenbereich und den Gruppentyp. Die Gruppenfamilie erstellt Gruppen mit dem Bereich und Typ, den Sie auswählen.

Ort der Gruppen

Auf der nächsten Seite können Sie den Container angeben, der die von der Gruppenfamilie generierten Gruppen enthalten soll.

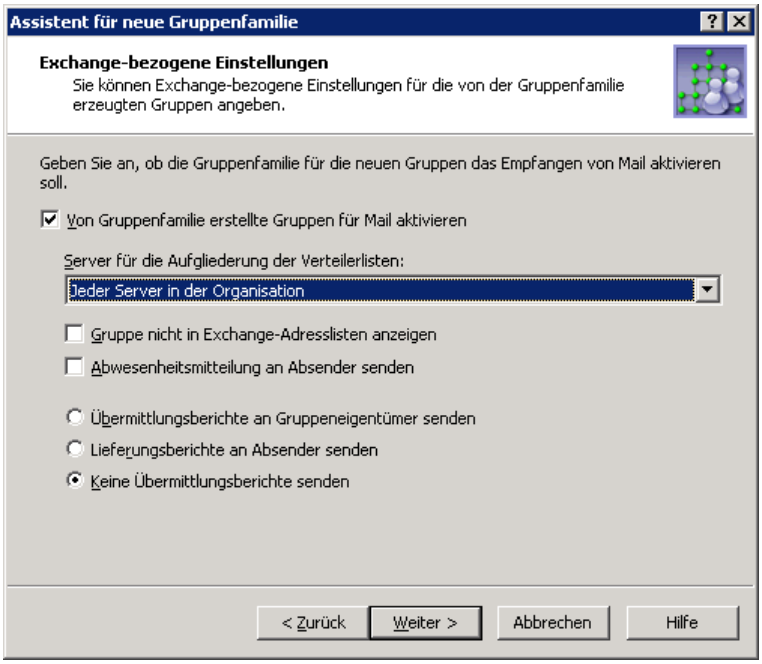

Assistent für neue Gruppenfamilie
Ort der Gruppen
Sie können den Container für die von der Gruppenfamilie erzeugten Gruppen angeben.
Wählen Sie den Container, in dem die Gruppenfamilie Gruppen erstellen soll.
Stammorganisationseinheit der Gruppenfamilie
Organisationseinheit, in der sich die Konfigurationsspeichergruppe der Gruppenfamilie befindet.
Diese Organisationseinheit:
Auswählen...
< Zurück
Weiter >
Abbrechen
Hilfe

Sie können eine der folgenden Optionen auswählen:

- **Stammorganisationseinheit der Gruppenfamilie** Die Gruppenfamilie erstellt Gruppen in dem Container, der die Konfigurationsspeichergruppe für diese Gruppenfamilie enthält (siehe „Starten des Assistenten für neue Gruppenfamilie" weiter oben in diesem Kapitel).
- **Diese Organisationseinheit** Die Gruppenfamilie erstellt Gruppen in dem angegebenen Container. Klicken Sie zur Auswahl eines Containers auf **Auswählen**.

Exchange-bezogene Einstellungen

Auf der nächsten Seite können Sie angeben, ob die von der Gruppenfamilie generierten Gruppen E-Mail-fähig sein sollen. Außerdem können Sie Eigenschaften im Zusammenhang mit Exchange einrichten, die diesen Gruppen bei ihrer Erstellung zugewiesen werden sollen.


Assistent für neue Gruppenfamilie
Exchange-bezogene Einstellungen
Sie können Exchange-bezogene Einstellungen für die von der Gruppenfamilie erzeugten Gruppen angeben.
Geben Sie an, ob die Gruppenfamilie für die neuen Gruppen das Empfangen von Mail aktivieren soll.
Von Gruppenfamilie erstellte Gruppen für Mail aktivieren
Server für die Aufgliederung der Verteilerlisten:
Jeder Server in der Organisation
Gruppe nicht in Exchange-Adresslisten anzeigen
Abwesenheitsmitteilung an Absender senden
Übermittlungsberichte an Gruppeneigentümer senden
Lieferungsberichte an Absender senden
Keine Übermittlungsberichte senden
< Zurück
Weiter >
Abbrechen
Hilfe

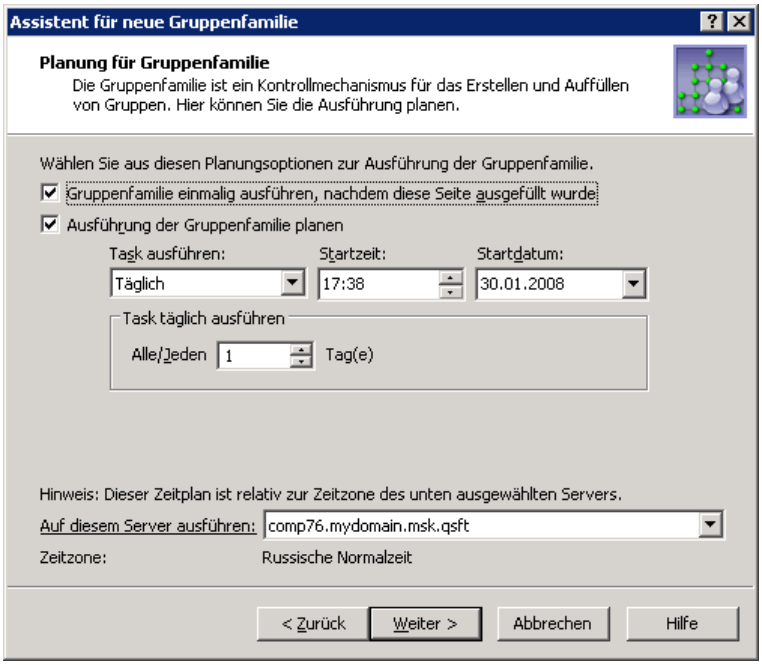
Wenn die Gruppen der Gruppenfamilie E-Mail-fähig sein sollen, aktivieren Sie das Kontrollkästchen **Von Gruppenfamilie erstellte Gruppen für Mail aktivieren**. Dann können Sie die folgenden Eigenschaften im Zusammenhang mit Exchange für die Gruppen der Gruppenfamilie einrichten:

- **Server für die Aufgliederung der Verteilerlisten** Der Exchange Server, mit dem eine Gruppe der Gruppenfamilie zu einer Liste von Gruppenmitgliedern erweitert wird.
- **Gruppe nicht in Exchange-Adresslisten anzeigen** Verhindert, dass die Gruppen der Gruppenfamilie in Adressenlisten angezeigt werden. Wenn Sie dieses Kontrollkästchen aktivieren, werden alle Gruppen in allen Adressenlisten ausgeblendet.
- **Abwesenheitsmitteilung an Absender senden** Aktivieren Sie dieses Kontrollkästchen, wenn Sie möchten, dass Abwesenheitsbenachrichtigungen an den Urheber der Nachricht gesendet werden, wenn eine Nachricht an eine Gruppe in der Gruppenfamilie gesendet wird und mindestens ein Gruppenmitglied eine Abwesenheitsbenachrichtigung aktiviert hat.
- **Übermittlungsberichte an Gruppeneigentümer senden** Verwenden Sie diese Option, wenn Sie möchten, dass Übermittlungsberichte an den Gruppenbesitzer gesendet werden, wenn eine Nachricht an eine Gruppe in der Gruppenfamilie nicht übermittelt werden kann. So wird der Gruppenbesitzer darüber informiert, dass die Nachricht nicht übermittelt wurde.
- **Lieferungsberichte an Absender senden** Verwenden Sie diese Option, wenn Sie möchten, dass Übermittlungsberichte an den Urheber der Nachricht gesendet werden, wenn eine Nachricht an eine Gruppe in der Gruppenfamilie nicht übermittelt werden kann. So wird der Urheber der Nachricht darüber informiert, dass die Nachricht nicht übermittelt wurde.
- **Keine Übermittlungsberichte senden** Verwenden Sie diese Option, wenn Sie nicht möchten, dass Übermittlungsberichte gesendet werden, selbst wenn eine Nachricht an eine Gruppenfamilie nicht übermittelt werden kann.

Planung für Gruppenfamilie

Auf der nächsten Seite können Sie die Ausführungen der Gruppenfamilie planen. Während jeder Ausführung verhält sich die Gruppenfamilie wie im Abschnitt „Funktionsweise" weiter oben in diesem Kapitel beschrieben.

Beachten Sie beim Einrichten der Zeitplanoptionen, dass eine Ausführung der Gruppenfamilie lange dauert und viele Ressourcen beansprucht. Daher sollte sie für einen Zeitraum geplant werden, in dem sie möglichst geringe Auswirkungen auf Benutzer hat.



Aktivieren Sie das erste Kontrollkästchen, um die Gruppenfamilie direkt nach Abschluss des Assistenten und immer dann, wenn die Gruppenfamilie durch die Verwaltung der Konfigurationsspeichergruppe geändert wird, auszuführen (siehe „Verwalten einer Gruppenfamilie" weiter unten in diesem Kapitel).

Aktivieren Sie das zweite Kontrollkästchen, um Zeitplanoptionen einzurichten. Wenn dieses Kontrollkästchen aktiviert ist, wird die Gruppenfamilie zu angegebenen Zeiten ausgeführt.

In der Liste **Auf diesem Server ausführen** können Sie den Verwaltungsdienst auswählen, mit dem die Gruppenfamilie ausgeführt werden soll. Sie sollten den Dienst mit der geringsten Auslastung auswählen.

Verwalten einer Gruppenfamilie

Die meisten Aufgaben im Zusammenhang mit der Gruppenfamilienverwaltung werden mit dem Befehl **Eigenschaften** für die Gruppen ausgeführt, in denen die Gruppenfamilienkonfigurationen gespeichert sind. Auf der ActiveRoles Server-Konsole sind solche Gruppen mit einem besonderen Symbol markiert, das sie von gewöhnlichen Gruppen unterscheidet.

Wenn Sie eine Gruppenfamilie erstellen, wird eine Gruppe erstellt, in der die Gruppenfamilien-konfiguration gespeichert wird. Der Gruppe wird der Name zugewiesen, den Sie für die Gruppenfamilie bereitgestellt haben, und sie wird mit dem Gruppenfamilien-Symbol markiert:

Um die Gruppenfamilienverwaltung zu erleichtern, enthält das Dialogfeld **Eigenschaften** für eine Konfigurationsspeichergruppe eine Reihe von Registerkarten speziell für Gruppenfamilien:

- **Allgemein** Zeigt den Namen der Gruppenfamilie an, und ermöglicht dem Administrator, die Beschreibung, den Gruppentyp und den Gruppenbereich der Speichergruppe anzuzeigen oder zu ändern.
- **Kontrollierte Gruppen** Listet die Gruppen auf, die von der Gruppenfamilie kontrolliert werden, und ermöglicht dem Administrator das Anzeigen und Ändern der Verknüpfungen zwischen Gruppe und Gruppierung sowie der Regeln im Zusammenhang mit der Gruppenerstellung.
- **Gruppierungen** Ermöglicht dem Administrator das Anzeigen oder Ändern des Gruppenfamilienbereichs und der Liste von Gruppieren-nach-Eigenschaften.
- **Zeitplan** Zeigt Informationen zum Zeitplan der Gruppenfamilie an und ermöglicht dem Administrator das Anzeigen oder Ändern von Zeitplanungseinstellungen.
- **Aktionsübersicht** Zeigt Informationen zur letzten Ausführung der Gruppenfamilie an und ermöglicht dem Administrator das Anzeigen eines detaillierten Protokolls zu den Ausführungsergebnissen.

Diese Registerkarten werden weiter unten in diesem Abschnitt detaillierter erörtert.

Änderungen an den gewöhnlichen, auf Gruppen bezogenen Eigenschaften der Konfigurationsspeicher-gruppe haben keine Auswirkungen auf die Gruppenfamilie. Beispielsweise können Sie die Konfigurations-speichergruppe umbenennen oder verschieben, ohne dass Auswirkungen auf den Prozess und die Ergebnisse eines Gruppenfamilienvorgangs entstehen. Wenn Sie die Konfigurationsspeichergruppe umbenennen, wird nur der Anzeigename der Gruppenfamilie geändert.

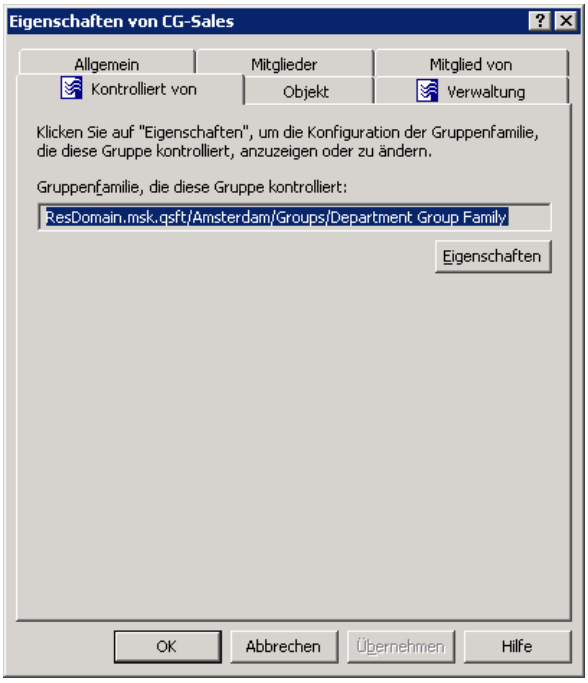
Das Menü **Aktion** in jeder Gruppenfamilien-Konfigurationsspeichergruppe enthält den Befehl **Ausführung erzwingen**, sodass Sie die Gruppenfamilie ausführen können, wenn Sie sie direkt aktualisieren möchten, ohne auf die geplante Ausführungszeit zu warten.

Kontrollierte Gruppen

Damit die Gruppen, die von einer Gruppenfamilie kontrolliert werden (die kontrollierten Gruppen) leichter zu erkennen sind, sind sie auf der ActiveRoles Server-Konsole mit einem besonderen Symbol markiert. So wird zum Beispiel das folgende Symbol verwendet, um eine globale Gruppe anzugeben, die unter der Kontrolle einer Gruppenfamilie steht:

Zusätzlich wird dem Feld **Hinweise** für solche Gruppen ein erklärender Text hinzugefügt, der angibt, dass die Gruppenfamilie alle Änderungen außer Kraft setzt, die direkt an der Gruppenmitgliedschaftsliste vorgenommen werden.

Auf der ActiveRoles Server-Konsole schließt das Dialogfeld **Eigenschaften** für kontrollierte Gruppen eine Registerkarte speziell für die Gruppenfamilie ein, die Registerkarte **Kontrolliert von**. Über diese Registerkarte können Sie die Konfiguration der Gruppenfamilie verwalten, die die Gruppe steuert:



Auf der Registerkarte **Kontrolliert von** werden der Pfad und der Name der Gruppenfamilien-Konfigurationsspeichergruppe angezeigt. Diese Registerkarte stellt einen Einstiegspunkt für die Gruppenfamilienverwaltung dar.

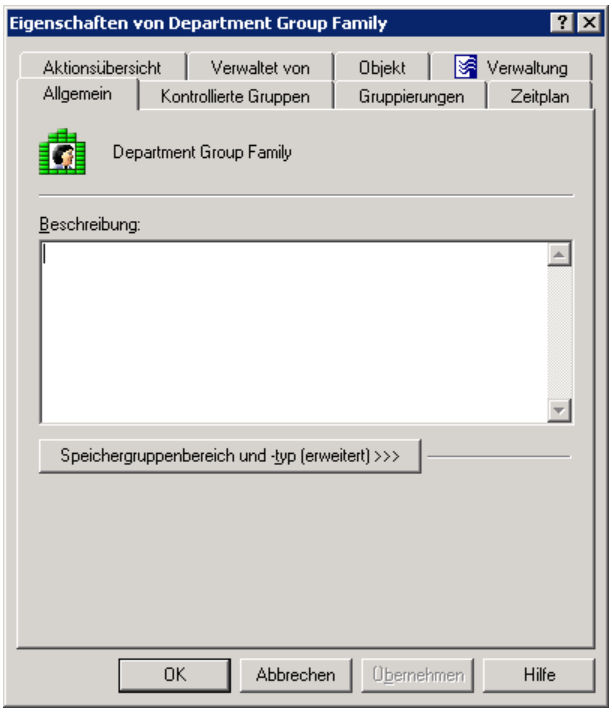
Es gibt also zwei Möglichkeiten, auf das Dialogfeld **Eigenschaften** der Gruppenfamilien-Konfigurationsspeichergruppe auf der ActiveRoles Server-Konsole zuzugreifen:

- Klicken Sie im Dialogfeld **Eigenschaften** für eine beliebige von der Gruppenfamilie kontrollierte Gruppe auf der Registerkarte **Kontrolliert von** auf **Eigenschaften**
- Klicken Sie mit der rechten Maustaste auf die Konfigurationsspeichergruppe, und klicken Sie dann auf **Eigenschaften**

In den folgenden Abschnitten werden die speziellen Registerkarten für die Gruppenfamilie erörtert, die im Dialogfeld **Eigenschaften** für die Konfigurationsspeichergruppe enthalten sind.

Registerkarte „Allgemein"

Auf der Registerkarte **Allgemein** wird der Name der Gruppenfamilie angezeigt. Außerdem können Sie hier ihre Beschreibung bearbeiten:

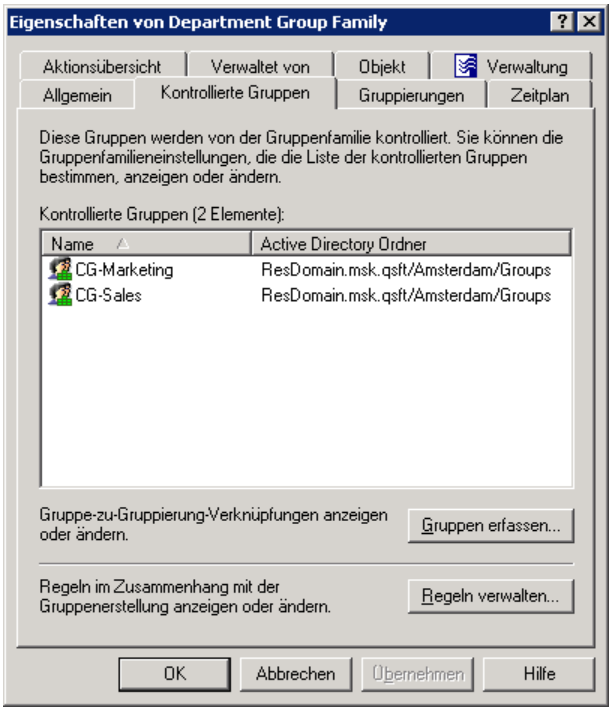


Der Name der Gruppenfamilie kann auf dieser Registerkarte nicht geändert werden. Verwenden Sie zum Ändern des Namens den Befehl **Umbenennen** für die Konfigurationsspeichergruppe.

Indem Sie auf **Speichergruppenbereich und -typ (erweitert)** klicken, können Sie den Bereich anzeigen, der zum Anzeigen und Ändern des Gruppenbereichs und des Gruppentyps der Konfigurationsspeichergruppe dient. Änderungen an diesen Einstellungen haben keine Auswirkungen auf die Gruppenfamilie. Der Gruppentyp und der Gruppenbereich sind standardmäßig auf den Sicherheitstyp und den globalen Bereich festgelegt. Normalerweise müssen sie nicht geändert werden.

Registerkarte „Kontrollierte Gruppen“

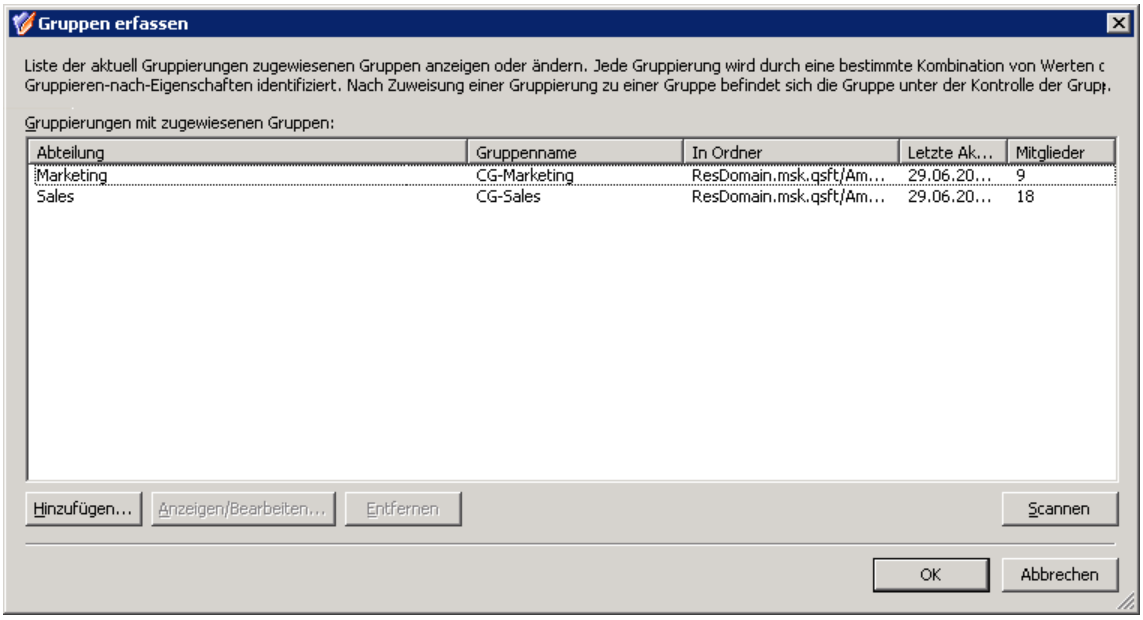
Auf der Registerkarte **Kontrollierte Gruppen** wird eine Liste der Gruppen angezeigt, die von der Gruppenfamilie kontrolliert werden:



Jede der aufgelisteten Gruppen wird von der Gruppenfamilie erstellt oder erfasst und mit einer bestimmten Gruppierung verknüpft. Sie können diese Verknüpfungen anzeigen oder ändern, wenn Sie auf **Gruppen erfassen** klicken.

Für eine neu erstellte Gruppenfamilienkonfiguration schließt die Liste auf dieser Tabelle nur die Gruppen ein, die im Schritt **Vorhandene Gruppen manuell erfassen** des Assistenten „Neue Gruppenfamilie“ angegeben wurde. Wenn dieser Schritt ausgelassen wurde, ist die Liste leer, bis die Gruppenfamilie mindestens einmal ausgeführt wurde.

Wenn Sie auf **Gruppen erfassen** klicken, wird ein Fenster angezeigt, in dem die Liste der kontrollierten Gruppen detaillierter angezeigt wird. Im Fenster **Gruppen erfassen** können Sie Einträge dieser Liste hinzufügen, ändern oder entfernen.



Im Fenster **Gruppen erfassen** werden alle kontrollierten Gruppen aufgelistet. Für jede Gruppe wird angezeigt, welche Gruppierung mit ihr verknüpft ist. Wie immer werden Gruppierungen durch Kombinationen von Werten der Gruppieren-nach-Eigenschaften identifiziert. Jeder Eintrag in der Liste schließt daher die folgenden Informationen ein:

- **Kombination von Werten der „Gruppieren-nach-Eigenschaften"** Die Kombination von Eigenschaftswerten, die eine Gruppierung identifiziert.
- **Gruppenname** Identifiziert die Gruppe, die mit der Gruppierung verknüpft ist.
- **In Ordner** Der kanonische Name des Containers, der die Gruppe enthält.
- **Letzte Aktualisierung** Das Datum und die Uhrzeit der letzten Aktualisierung dieser Gruppe durch die Gruppenfamilie. Die Aktualisierung tritt während einer Ausführung der Gruppenfamilie auf. Dabei werden ggf. alle Änderungen an der Gruppierung erkannt, und die Mitgliedschaftsliste der Gruppe wird so geändert, dass sie diese Änderungen widerspiegelt.
- **Mitglieder** Die Anzahl der Mitglieder in der Gruppe nach der letzten Aktualisierung. Diese entspricht der Anzahl der Objekte, die die Gruppenfamilie zum Zeitpunkt der letzten Aktualisierung in der Gruppierung gefunden hat.

Im Fenster **Gruppen erfassen** stehen folgende Schaltflächen zum Verwalten der Liste zur Verfügung:

- **Hinzufügen** Öffnet ein Fenster, in dem Sie eine vorhandene Gruppe auswählen und eine Gruppierung angeben können, mit der die Gruppe verknüpft (ihr zugewiesen) werden soll. Um eine Gruppierung anzugeben, müssen Sie einen bestimmten Wert jeder der Gruppieren-nach-Eigenschaften eingeben. Dann wird die ausgewählte Gruppe mit der Gruppierung verknüpft, die durch die eingegebene Wertekombination identifiziert wird.
- **Anzeigen/Bearbeiten** Ermöglicht das Ändern eines Eintrags, den Sie in der Liste auswählen. Öffnet ein Fenster, in dem Sie eine andere Gruppe auswählen können oder eine andere Gruppierung angeben können, indem Sie die Wertekombination der Gruppieren-nach-Eigenschaften ändern.

- **Entfernen** Löscht die ausgewählten Einträge aus der Liste. Die Gruppenfamilie erstellt dann neue Gruppen für die Gruppierungen, die Sie aus der Liste entfernt haben.
- **Scannen** Erkennt neue Kombinationen von „Gruppieren-nach-Eigenschaften" und zeigt diese in der Liste an, sodass Sie sie mit vorhandenen Gruppen zu einer neuen Kombination verknüpfen können, wenn die Gruppenfamilie nicht neue Gruppen für diese Kombinationen erstellen soll.

Beachten Sie Folgendes bei der Verwaltung der Gruppenliste im Fenster **Gruppen erfassen**:

- Sie können eine vorhandene Gruppe einer Gruppierung unabhängig davon zuweisen, ob die Gruppierung im Verzeichnis tatsächlich vorhanden ist. Sie können beispielsweise eine Gruppe einer Gruppierung mit einem Wert für die Abteilungseigenschaft zuweisen, der im Verzeichnis nicht enthalten ist. Wenn die Abteilungseigenschaft für Benutzer auf diesen Wert festgelegt wird, fügt die Gruppenfamilie diese Benutzer der angegebenen Gruppe hinzu, statt für die neue Abteilung eine neue Gruppe zu erstellen.
- Jeder Gruppierung kann nur eine einzige Gruppe zugewiesen werden. Wenn die Liste eine bestimmte Gruppierung bereits enthält, können Sie keinen neuen Eintrag hinzufügen, der auf dieselbe Gruppierung verweist. In diesem Fall können Sie die Schaltfläche **Bearbeiten** verwenden, um eine andere Gruppe mit der Gruppierung zu verknüpfen.
- Wenn Sie einen Listeneintrag bearbeiten, um eine andere Gruppe mit einer Gruppierung zu verknüpfen, bleibt die zuvor mit der Gruppierung verknüpfte Gruppe unverändert. Sie wird nicht gelöscht, und ihre Mitgliedschaftsliste wird nicht aktualisiert. Die Mitglieder dieser Gruppierung gehören also immer noch zu der Gruppe, obwohl Sie die Gruppe aus der Liste entfernt haben und sie somit nicht mehr von der Gruppenfamilie kontrolliert wird.
- Wenn Sie einen Eintrag aus der Liste entfernen, wird die Gruppe, auf die er verweist, nicht gelöscht. Während einer späteren Ausführung erkennt die Gruppenfamilie eine Gruppierung, der keine Gruppe zugewiesen ist, und versucht, eine Gruppe für sie zu erstellen. Dieser Vorgang kann aufgrund eines Namenskonflikts fehlschlagen, wenn eine Gruppe mit demselben Namen vorhanden ist, also die Gruppe, die zuvor mit der Gruppierung verknüpft war. Um Namenskonflikte zu vermeiden, sollten Sie die Gruppen, die Sie aus der Kontrolle der Gruppenfamilie entfernen, umbenennen oder löschen.

Regeln im Zusammenhang mit der Gruppenerstellung

Wenn eine Gruppenfamilie eine Gruppierung erkennt, die nicht mit einer Gruppe verknüpft ist, erstellt sie eine neue Gruppe, verknüpft die neue Gruppe mit der Gruppierung und fügt ihr Mitglieder der Gruppierung hinzu. Die Gruppenfamilienkonfiguration gibt eine Reihe von Regeln für das Einrichten bestimmter Eigenschaften für neue Gruppen an.

Die Regeln, die den Gruppenerstellungsprozess steuern, werden bei der Erstellung der Gruppenfamilien-konfiguration definiert. Um diese Regeln zu untersuchen oder zu ändern, verwenden Sie im Dialogfeld **Eigenschaften** der Gruppenfamilienkonfigurations-Speichergruppe auf der Registerkarte **Kontrollierte Gruppen** die Schaltfläche **Regeln verwalten**.

Über die Schaltfläche **Regeln verwalten** haben Sie Zugriff auf eine Reihe von Seiten, die denen des Assistenten „Neue Gruppenfamilie" ähneln. Dieser Assistent wird weiter oben in diesem Kapitel diskutiert. Wenn Sie auf **Regeln verwalten** klicken, wird ein schrittweiser Vorgang gestartet, der folgende Seiten umfasst:

- **Gruppenbenennungsregel** Die Gruppenfamilie verwendet diese Regel bei der Erstellung neuer Gruppen zum Generieren folgender Werte: Gruppenname, Anzeigename, Gruppenname (Prä-Windows 2000) und E-Mail-Alias. Details finden Sie Abschnitt „Gruppenbenennungsregel" weiter oben in diesem Kapitel.
- **Gruppenbereich und -typ** Der Gruppentyp und der Gruppenbereich, die den von der Gruppenfamilie erstellten Gruppen zugewiesen werden.
- **Ort der Gruppen** Die Regel, die bestimmt, in welchem Container die Gruppenfamilie neue Gruppen erstellt. Details finden Sie Abschnitt „Speicherort von Gruppen" weiter oben in diesem Kapitel.
- **Exchange-bezogene Einstellungen** Die Regel, die bestimmt, ob die von der Gruppenfamilie erstellten Gruppen E-Mail-fähig sind. Außerdem legt diese Regel eine Reihe von Optionen für E-Mail-fähige Gruppen fest. Details finden Sie Abschnitt „Exchange-bezogene Einstellungen" weiter oben in diesem Kapitel.

Sie können mit Hilfe der Schaltflächen **Zurück** und **Weiter** durch diese Seiten navigieren. Mit der Schaltfläche **Fertig stellen** auf der letzten Seite werden ggf. die Änderungen von allen Seiten im Dialogfeld **Eigenschaften** festgeschrieben, und die Verwaltungsaufgabe für die Gruppenerstellungsregeln wird abgeschlossen. Die Änderungen werden übernommen, wenn Sie im Dialogfeld **Eigenschaften** auf **OK** oder **Anwenden** klicken. Wenn Sie sie verwerfen möchten, klicken Sie auf **Abbrechen**.

Registerkarte „Gruppierungen"

Über die Registerkarte **Gruppierungen** können Sie auf die Benutzeroberfläche zum Konfigurieren der Gruppenfamilieneinstellungen zugreifen, die den Berechnungsprozess für Gruppierungen steuern.

Während jeder Ausführung berechnet die Gruppenfamilie Gruppierungen neu. Dazu zerlegt sie die Menge der verwalteten Objekte (den Bereich) in Teilmengen. Jede Teilmenge besteht aus den Objekten, für die jeder der Gruppieren-nach-Eigenschaften ein bestimmter Wert zugewiesen ist.

Die Einstellungen, die den Bereich und die Gruppieren-nach-Eigenschaften bestimmen, werden bei der Erstellung der Gruppenfamilienkonfiguration definiert. Sie können diese Einstellungen mit Hilfe der Schaltfläche **Konfigurieren** auf der Registerkarte **Gruppierungen** untersuchen oder ändern.

Über die Schaltfläche **Konfigurieren** haben Sie Zugriff auf eine Reihe von Seiten, die denen des Assistenten „Neue Gruppenfamilie" ähneln. Dieser Assistent wird weiter oben in diesem Kapitel diskutiert. Wenn Sie auf **Konfigurieren** klicken, wird ein schrittweiser Vorgang gestartet, der folgende Seiten umfasst:

- **Ort der verwalteten Objekte** Die Verzeichniscontainer, in denen die Gruppenfamilie nach Objekten sucht, die in den Bereich eingeschlossen werden sollen. Details finden Sie Abschnitt „Speicherort von verwalteten Objekten" weiter oben in diesem Kapitel.
- **Auswahl der verwalteten Objekte** Die Kriterien, mit denen die Gruppenfamilie bestimmt, ob das jeweilige Objekt in den Bereich eingeschlossen werden soll. Details finden Sie Abschnitt „Auswahl von verwalteten Objekten" weiter oben in diesem Kapitel.
- **Gruppieren-nach-Eigenschaften** Die Liste der Eigenschaften, mit denen die Gruppenfamilie Gruppierungen berechnet. Details finden Sie Abschnitt „Gruppieren-nach-Eigenschaften" weiter oben in diesem Kapitel.

Sie können mit Hilfe der Schaltflächen **Zurück** und **Weiter** durch diese Seiten navigieren. Mit der Schaltfläche **Fertig stellen** auf der letzten Seite werden ggf. die Änderungen von allen Seiten im Dialogfeld **Eigenschaften** festgeschrieben, und die Verwaltungsaufgabe für die Gruppierungs-berechnungsregeln wird abgeschlossen. Die Änderungen werden übernommen, wenn Sie im Dialogfeld **Eigenschaften** auf **OK** oder **Anwenden** klicken. Wenn Sie sie verwerfen möchten, klicken Sie auf **Abbrechen**.

Wenn Sie die Änderungen an der Liste auf der Seite **Gruppieren-nach-Eigenschaften** übernommen haben, legen Sie die Gruppenfamilienoptionen neu fest, die von den Gruppieren-nach-Eigenschaften abhängig sind. Zu diesen Optionen gehören die Gruppenbenennungsregeln und die Liste der zu erfassenden Gruppen. Wenn Sie eine Gruppieren-nach-Eigenschaft hinzufügen oder entfernen, werden die aktuellen Benennungsregeln durch die Standardbenennungsregel ersetzt, und die Liste der zu erfassenden Gruppen wird gelöscht.

Registerkarte „Zeitplan"

Die Registerkarte **Zeitplan** zeigt Informationen zum Zeitplan der Gruppenfamilie an und ermöglicht Ihnen das Anzeigen oder Ändern von Zeitplanungseinstellungen.

Auf der Registerkarte werden die folgenden Informationen angezeigt:

- **Zeitplan** Für die Gruppenfamilie wird die Ausführung anhand dieser Anweisung geplant.
- **Auf diesem Server ausführen** Der Verwaltungsdienst, der alle für die Ausführung der Gruppenfamilie notwendigen Vorgänge ausführt.
- **Letzte Laufzeit** Das Datum und die Uhrzeit der letzten Ausführung der Gruppenfamilie.
- **Nächste Ausführungszeit** Das Datum und die Uhrzeit der geplanten nächsten Ausführung der Gruppenfamilie.

Über die Schaltfläche **Konfigurieren** können Sie den Zeitplan der Gruppenfamilie detaillierter untersuchen und ihn nach Bedarf anpassen.

Durch Anklicken von **Konfigurieren** wird die Seite **Planung für Gruppenfamilie** angezeigt, die der des Assistenten „Neue Gruppenfamilie", der weiter oben in diesem Kapitel beschrieben wurde (siehe Abschnitt „Gruppenfamilienplanung") ähnelt. Betrachten oder ändern Sie die Zeitplaneinstellungen auf dieser Seite, und klicken Sie auf die Schaltfläche **Fertig stellen**, um Ihre Änderungen im Dialogfeld **Eigenschaften** festzuschreiben. Die Änderungen werden übernommen, wenn Sie auf die Schaltfläche **OK** oder **Anwenden** klicken. Wenn Sie sie verwerfen möchten, klicken Sie auf **Abbrechen**.

Registerkarte „Vorgangsübersicht"

Auf der Registerkarte **Aktionsübersicht** werden quantitative Informationen zur Ausführung der Gruppenfamilie angezeigt.

Auf der Registerkarte **Aktionsübersicht** werden folgende Informationen zur letzten Ausführung der Gruppenfamilie angezeigt:

- **Letzte Ausführung gestartet** Das Datum und die Uhrzeit des Ausführungsstarts.
- **Letzte Ausführung beendet** Das Datum und die Uhrzeit des Ausführungsendes.
- **Verwaltete Objekte** Die Anzahl der Objekte, die im Bereich der Gruppenfamilie gefunden wurden.
- **Gültige Gruppierungen** Die Anzahl der Gruppierungen, die während der Ausführung berechnet wurden.
- **Fehlerhafte Gruppierungen** Die Anzahl der Gruppierungen, die die Gruppenfamilie nicht identifizieren konnte, weil ihre Gruppieren-nach-Eigenschaften ungültige Wertekombinationen aufweisen. Beispielsweise tritt eine ungültige Kombination auf, wenn Werte für mindestens eine Eigenschaft in der Kombination fehlen.
- **Erstellte Gruppen** Die Anzahl der Gruppen, die die Gruppenfamilie während der Ausführung erstellt hat.
- **Aktualisierte Gruppen** Die Anzahl der Gruppen, für die die Gruppenfamilie während der Ausführung die Mitgliedschaftslisten aktualisiert hat.
- **Aktualisierungen in Gruppenmitgliedschaften** Die Anzahl der Objekte, die die Gruppenfamilie während der Ausführung zu Gruppen hinzugefügt oder aus Gruppen entfernt hat.
- **Fehler** Die Anzahl der Fehler während der Ausführung.

Um diese Informationen genauer zu untersuchen, klicken Sie auf die Schaltfläche **Protokoll anzeigen**.

Vorgangsübersicht-Protokoll

Wenn Sie auf die Schaltfläche **Protokoll anzeigen** klicken, wird ein Protokoll mit Zusammenfassungsinformationen zur letzten Ausführung der Gruppenfamilie angezeigt. Das Protokoll enthält ggf. Beschreibungen der Fehlersituationen, die während der Ausführung aufgetreten sind, und fasst die quantitativen Ergebnisse der Ausführung zusammen, z.B. die Anzahl aktualisierter Gruppen, die Anzahl erstellter Gruppen und die Anzahl der Objekte, deren Gruppenmitgliedschaften geändert wurden.

Das Protokoll besteht aus drei Abschnitten: Prolog, Fehlerliste und Epilog. Die Abschnitte „Prolog" und „Epilog" sind immer im Protokoll enthalten. Dagegen ist die „Fehler Liste" nur dann vorhanden, wenn bei der Ausführung Fehler oder Warnungen aufgetreten sind.

Der Abschnitt „Prolog" bietet die folgenden Informationen:

- Das Datum und die Uhrzeit des Ausführungsstarts
- Die Anzahl der verwalteten Objekte, die im Bereich der Gruppenfamilie gefunden wurden
- Die Gesamtanzahl der Gruppierungen, die durch Analyse der Gruppieren-nach-Eigenschaften gefunden wurden

Der Abschnitt „Epilog" bietet die folgenden Informationen:

- Ggf. die Anzahl der Fehler
- Ggf. die Anzahl ungültiger Wertekombinationen von Gruppieren-nach-Eigenschaften
- Die Anzahl der Gruppen, die die Gruppenfamilie während der Ausführung erstellt hat
- Die Anzahl der Gruppen, die die Gruppenfamilie während der Ausführung aktualisiert hat

Der Fehler Liste enthält Informationen zu allen Fehlern und Warnungen, die während der Ausführung der Gruppenfamilie aufgetreten sind.

Szenario: Abteilungsbezogene Gruppenfamilie

Um die Ausführung der Gruppenfamilienfunktionen zu sehen, können Sie das folgende Szenario durchlaufen.

Angenommen, die Organisationseinheit (Organizational Unit, OU) für Benutzer enthält eine Reihe von Benutzerkonten. Nehmen Sie außerdem an, dass sich für jeden der unten aufgelisteten Werte mindestens ein Konto in der Organisationseinheit für Benutzer befindet, das diesen Wert als Abteilungseigenschaft aufweist. Die folgenden Werte der Abteilungseigenschaft finden sich für die Benutzerkonten in der Organisationseinheit für die Benutzer:

- Accounting (Buchhaltung)
- Educational Services (Bildung)
- Executive Services (Personaldienstleistungen)
- Facilities (Versorgungsaufgaben)
- Finance (Finanzen)
- Government Services (behördliche Dienste)
- Human Resources (Personalabteilung)
- Information Technology (IT)
- International Services (internationale Dienstleistungen)
- Operations (Betrieb)

In diesem Abschnitt finden Sie Anweisungen zum Implementieren einer Gruppenfamilie, die für die Benutzer in jeder diese Abteilungen eine eigene Gruppe erstellt und pflegt. Die Gruppenfamilien-Konfigurationsspeichergruppe wird in der Organisationseinheit für Gruppen erstellt. Die Gruppenfamilie wird so konfiguriert, dass sie die Abteilungsgruppen in derselben Organisationseinheit erstellt.

Öffnen Sie die ActiveRoles Server-Konsole, und führen Sie die folgenden Schritte aus, um die Gruppenfamilie zu implementieren.

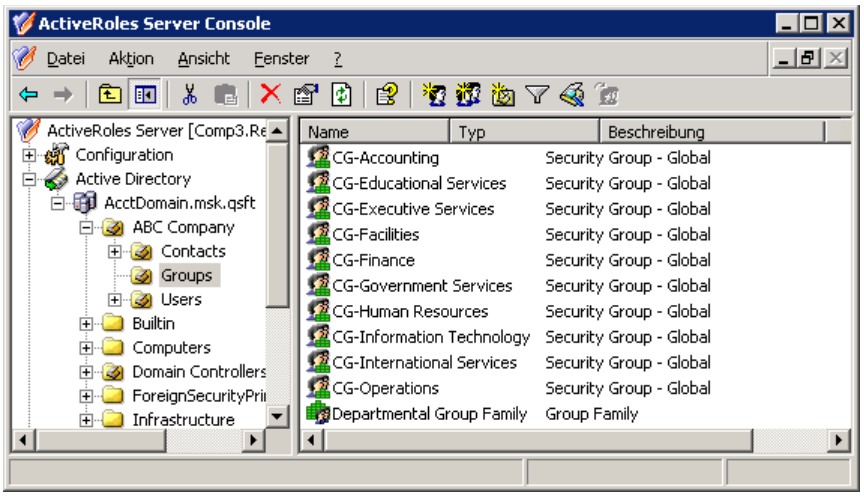
So erstellen Sie die abteilungsbezogene Gruppenfamilie und führen sie aus:

1. Klicken Sie mit der rechten Maustaste auf die Organisationseinheit **Gruppen**, und klicken Sie dann auf **Neu | Gruppenfamilie**.
   Hierdurch wird der Assistent „Neue Gruppenfamilie" gestartet. Die übrigen Schritte gelten für diesen Assistenten.
2. Klicken Sie auf der Seite Willkommen auf **Weiter**.

3. Geben Sie in das Feld **Name der Gruppenfamilie** den Wert **abteilungsbezogene Gruppenfamilie** ein. Klicken Sie auf **Weiter**.
4. Klicken Sie auf die Option **Vorkonfigurierte Gruppierung nach**, klicken Sie in der Liste unter dieser Option auf **Department**, und klicken Sie dann auf **Weiter**.
5. Entfernen Sie die Organisationseinheit **Gruppen** aus der Liste **Container**, und fügen Sie der Liste die Organisationseinheit **Benutzer** hinzu. Klicken Sie auf **Weiter**.
6. Klicken Sie auf die Option **Benutzer** und dann auf **Weiter**.
7. Stellen Sie sicher, dass die Liste **Nach diese Eigenschaften gruppieren** nur einen Eintrag enthält, nämlich **Department**. Klicken Sie auf **Weiter**.
8. Aktivieren Sie das Kontrollkästchen **Diesen Schritt ohne manuelle Gruppenerfassung überspringen**. Klicken Sie auf **Weiter**.
9. Klicken Sie auf **Weiter**, um die Standardregel für die Gruppenbenennung zu akzeptieren: **CG-%<Schlüssel.Abteilung>**
10. Klicken Sie auf **Weiter**, um den Standardbereich und den Standardtyp für die Gruppe zu akzeptieren.
11. Klicken Sie auf **Weiter**, um den Standardspeicherort für die kontrollierten Gruppen zu akzeptieren: **Stammorganisationseinheit der Gruppenfamilie**.
12. Klicken Sie auf **Weiter**, um die Standardeinstellungen in Bezug auf Exchange zu akzeptieren.
13. Aktivieren Sie das Kontrollkästchen **Gruppenfamilie einmal nach Fertigstellung dieser Seite ausführen**. Klicken Sie auf **Weiter**.
14. Klicken Sie auf **Fertig stellen**.

Nachdem Sie diese Schritte abgeschlossen haben, führt die Gruppenfamilie die gesamte notwendige Verarbeitung zur Erstellung der Gruppen aus, eine Gruppe pro Abteilung, und fügt Benutzer anhand ihrer Abteilungseigenschaft den entsprechenden Gruppen hinzu.

Sie können sich den Inhalt der Organisationseinheit für Gruppen ansehen, um zu überprüfen, ob die Abteilungsgruppen erfolgreich erstellt wurden. Die Gruppenliste sollte der folgenden Abbildung ähneln:



Sie können auch Eigenschaften einer von der Gruppenfamilie generierten Gruppe untersuchen, um zu überprüfen, ob die Mitgliedschaftsliste der Gruppe richtig ist. Beispielsweise besteht die Mitgliedschaftsliste der Gruppe **CG-Executive Services (Personaldienstleistungen)** aus den Benutzerkonten, für die die Eigenschaft **Department** auf **Executive Services (Personaldienstleistungen)** festgelegt ist.

10

Dynamische Gruppen

- Grundlegendes zu dynamischen Gruppen
- Richtlinie zu dynamischen Gruppen
- Verwalten dynamischer Gruppen
- Szenario: Automatisches Verschieben von Benutzern zwischen Gruppen

Grundlegendes zu dynamischen Gruppen

In Active Directory können Gruppen (hier als Standardgruppen bezeichnet) Mitglieder statisch enthalten. Sie können also Objekte auswählen und sie den Gruppen hinzufügen. ActiveRoles Server stellt einen flexiblen, regelorientierten Mechanismus zum Auffüllen von Gruppen bereit. Nachdem dieser Prozess eingerichtet ist, fügt er automatisch Mitglieder zu Gruppen hinzu und entfernt sie daraus.

ActiveRoles Server stellt regelorientierte Gruppen bereit, die als dynamische Gruppen bezeichnet werden. Mitgliedschaftsregeln bestimmen, ob ein Objekt Mitglied einer dynamischen Gruppe ist. Eine Mitgliedschaftsregel kann die Form einer Suchabfrage, einer Regel für die statische Einschließung und Ausschließung von Objekten sowie einer Regel für die Einschließung und Ausschließung von Gruppenmitgliedern haben. Wenn die Umgebung verändert wird, werden die Mitgliedschaften von Objekten in dynamischen Gruppen automatisch geändert, um an die neue Umgebung angepasst zu werden.

Dynamische Gruppen von ActiveRoles Server reduzieren die Kosten für die Pflege von Listen und Gruppen und erhöhen zugleich die Genauigkeit und Zuverlässigkeit dieser Pflege. Außerdem werden Verteilerlisten und Sicherheitsgruppen automatisch aktuell gehalten, sodass Mitglieder nicht manuell hinzugefügt und entfernt werden müssen.

Um die Pflege von Gruppenmitgliedschaftslisten zu automatisieren, stellen dynamische Gruppen die folgenden Funktionen bereit:

- Regelorientierte Mechanismen, die automatisch Objekte zu Gruppen hinzufügen und aus ihnen entfernen, wenn Objektattribute in Active Directory geändert werden.
- Flexible Mitgliedschaftskriterien, die sowohl das abfragebasierte als auch das statische Füllen von Gruppen ermöglichen.

Auf der ActiveRoles Server-Konsole, werden dynamische Gruppen mit dem folgenden Symbol markiert: .

Wenn Sie eine Standardgruppe in eine dynamische Gruppe konvertieren, verliert die Gruppe alle Mitglieder, die zur Gruppe hinzugefügt worden sind, als diese noch eine Standardgruppe war. Der Grund ist, dass Mitglieder einer dynamischen Gruppe nur über Mitgliedschaftsregeln definiert werden können.

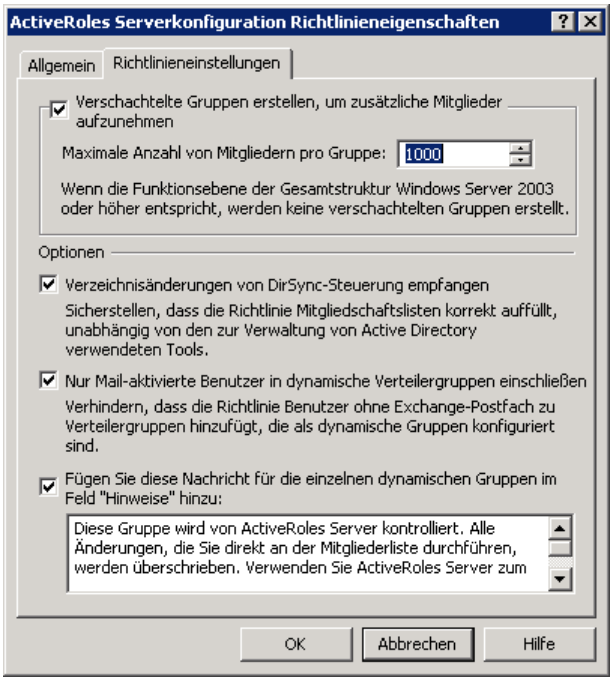
Wenn Sie eine dynamische Gruppe in eine Standardgruppe konvertieren, behält die Gruppe alle ihre Mitglieder, die aufgrund der Mitgliedschaftsregeln in sie eingeschlossen sind, verliert jedoch die Mitgliedschaftsregeln.

Wenn ein Mitglied einer dynamischen Gruppe wie etwa einer Benutzer- oder anderen Gruppe deprovisioniert ist, wird die dynamische Gruppe automatisch so aktualisiert, dass sie dieses Mitglied nicht mehr enthält. Folglich werden bei der Deprovisionierung eines Benutzers oder einer Gruppe dieser Benutzer oder diese Gruppe aus allen dynamischen Gruppen entfernt. Dieses Verhalten ist Absicht.

Richtlinie zu dynamischen Gruppen

Das Verhalten des Mechanismus für dynamische Gruppen wird von der Richtlinie definiert, die im integrierten Richtlinienobjekt „dynamische Gruppen" definiert ist. Mit dieser Richtlinie wird sichergestellt, dass alle mit einem beliebigen anderen Active Directory-Verwaltungstool an einer dynamischen Gruppe vorgenommenen Änderungen verworfen werden. Mitgliedschaftslisten können nur mit den Mitgliedschaftsregeln von ActiveRoles Server geändert werden.

Um die Richtlinie anzuzeigen oder zu ändern, rufen Sie das Dialogfeld **Eigenschaften** für das Richtlinienobjekt **Built-in Policy – Dynamic Groups** (im Container **Configuration/Policies/Administration/Builtin**) und dann die Registerkarte **Richtlinien** auf, wählen Sie die Richtlinie aus und klicken Sie dann auf **Anzeigen/Bearbeiten**. Nun wird das Dialogfeld **Richtlinieneigenschaften** angezeigt. Die Registerkarte **Richtlinieneinstellungen** im Dialogfeld **Richtlinieneigenschaften** sollte der folgenden Abbildung entsprechen.


ActiveRoles Serverkonfiguration Richtlinieneigenschaften
Allgemein
Richtlinieneinstellungen
Verschachtelte Gruppen erstellen, um zusätzliche Mitglieder aufzunehmen
Maximale Anzahl von Mitgliedern pro Gruppe:
1000
Wenn die Funktionsebene der Gesamtstruktur Windows Server 2003 oder höher entspricht, werden keine verschachtelten Gruppen erstellt.
Optionen
Verzeichnisänderungen von DirSync-Steuerung empfangen
Sicherstellen, dass die Richtlinie Mitgliedschaftslisten korrekt auffüllt, unabhängig von den zur Verwaltung von Active Directory verwendeten Tools.
Nur Mail-aktivierte Benutzer in dynamische Verteilergruppen einschließen
Verhindern, dass die Richtlinie Benutzer ohne Exchange-Postfach zu Verteilergruppen hinzufügt, die als dynamische Gruppen konfiguriert sind.
Fügen Sie diese Nachricht für die einzelnen dynamischen Gruppen im Feld "Hinweise" hinzu:
Diese Gruppe wird von ActiveRoles Server kontrolliert. Alle Änderungen, die Sie direkt an der Mitgliederliste durchführen, werden überschrieben. Verwenden Sie ActiveRoles Server zum
OK
Abbrechen
Hilfe

Auf der Registerkarte **Richtlinieneinstellungen** können Sie die folgenden Optionen einrichten:

- **Maximale Anzahl von Mitgliedern pro Gruppe** Gibt die maximal zulässige Anzahl von Mitgliedern einer dynamischen Gruppe an. Wenn die Mitgliedschaftsliste einer dynamischen Gruppe diesen Grenzwert überschreitet, erstellt ActiveRoles Server zusätzliche Gruppen, um die verbleibenden Mitglieder aufzunehmen, und fügt diese Gruppen zur dynamischen Gruppe hinzu.

  Wenn ActiveRoles Server keine verschachtelten Gruppen erstellen soll, deaktivieren Sie das Kontrollkästchen **Verschachtelte Gruppen erstellen, um zusätzliche Mitglieder aufzunehmen**. Wenn dieses Kontrollkästchen deaktiviert ist, ermöglicht die Richtlinie, dass dynamische Gruppen jede beliebige Anzahl von Mitgliedern enthalten können.

  Für dynamische Gruppen in Domänen, deren Gesamtstruktur-Funktionsebene auf Windows Server 2003 oder höher gesetzt ist, werden keine verschachtelten Gruppen erstellt. In diesem Fall ermöglicht die Richtlinie unabhängig vom Status des Kontrollkästchens, dass eine dynamische Gruppe jede beliebige Anzahl von Mitgliedern enthält.

- **Verzeichnisänderungen von der DirSync-Steuerung empfangen** Stellt sicher, dass die Richtlinie unabhängig davon, welche Tools für die Verwaltung von Active Directory verwendet werden, die Mitgliedschaftslisten richtig auffüllt. Wenn dieses Kontrollkästchen nicht aktiviert ist, sind einige regelorientierte Mitgliedschaftslisten möglicherweise mit Mitgliedschaftsregeln inkompatibel. In diesem Fall wendet die Richtlinie Mitgliedschaftsregeln nur dann neu an, wenn mit ActiveRoles Server Änderungen am Verzeichnis vorgenommen werden.
- **Nur Mail-aktivierte Benutzer in dynamische Verteilergruppen einschließen** Verhindert, dass die Richtlinie Benutzer ohne Exchange-Postfach zu Verteilergruppen hinzufügt, die als dynamische Gruppen konfiguriert sind.
- **Fügen Sie diese Nachricht für die einzelnen dynamischen Gruppen im Feld „Hinweise" hinzu** Legt den Nachrichtentext in der Eigenschaft **Hinweise** jeder dynamischen Gruppe ab. (Die Eigenschaft **Hinweise** wird im Dialogfeld **Eigenschaften** für die Gruppe auf der Registerkarte **Allgemein** angezeigt.)

Verwalten dynamischer Gruppen

In diesem Abschnitt wird die Administration dynamischer Gruppen mit der ActiveRoles Server-Konsole vorgestellt. Die folgenden Themen werden behandelt:

- Konvertieren einer Standardgruppe in eine dynamische Gruppe
- Anzeigen der Mitglieder einer dynamischen Gruppe
- Hinzufügen einer Mitgliedschaftsregel zu einer dynamischen Gruppe
- Entfernen einer Mitgliedschaftsregel aus einer dynamischen Gruppe
- Konvertieren einer dynamischen Gruppe in eine Standardgruppe
- Ändern, Löschen und Umbenennen einer dynamischen Gruppe

Konvertieren einer Standardgruppe in eine dynamische Gruppe

Klicken Sie zum Konvertieren einer Standardgruppe in eine dynamische Gruppe mit der rechten Maustaste auf die Gruppe und klicken Sie dann auf **In dynamische Gruppe konvertieren**, um den Assistenten „Neue Mitgliedschaftsregel" zu starten. Die erste Seite des Assistenten entspricht der folgenden Abbildung.

Assistent für neue Mitgliedschaftsregel
Typ der Mitgliedschaftsregel wählen:
Regeltyp
Beschreibung
Explizit einschließen
Objekts statisch einschließen
Nach Abfrage einschli...
Von Abfrage zurückgegebene Objekte einschli...
Gruppenmitglieder ein...
Mitglieder gewählter Gruppen einschließen
Explizit ausschließen
Objekte statisch ausschließen
Nach Abfrage ausschl...
Von Abfrage zurückgegebene Objekte ausschli...
Gruppenmitglieder au...
Mitglieder gewählter Gruppen ausschließen
Beschreibung der Mitgliedschaftsregel:
Objekte zum Hinzufügen zur Mitgliedschaftsliste wählen.
ActiveRoles Server stellt sicher, dass die gewählten Objekte in der Mitgliedschaftsliste enthalten sind, unabhängig davon, ob sie umbenannt, in einen anderen Container verschoben oder ihre Eigenschaften geändert
< Zurück
Weiter >
Abbrechen
Hilfe

Auf der ersten Seite des Assistenten können Sie den Typ der zu konfigurierenden Mitgliedschaftsregel auswählen. Im Text unter **Beschreibung der Mitgliedschaftsregel** wird erläutert, welche Mitgliedschaftsregeln mit dem ausgewählten Regeltyp erstellt werden können.

Mit der Mitgliedschaftsregel **Explizit einschließen** können Sie Objekte auswählen, die der Gruppe statisch hinzugefügt werden sollen. ActiveRoles Server stellt sicher, dass die ausgewählten Objekte auch dann in die Gruppe eingeschlossen sind, wenn sie umbenannt oder in einen anderen Container verschoben werden oder wenn ihre Eigenschaften geändert werden. Mit dem Regeltyp **Explizit einschließen** verhält sich die dynamische Gruppe wie eine Standardgruppe.

Mit der Mitgliedschaftsregel **Nach Abfrage einschließen** können Sie Kriterien definieren, die die Objekte erfüllen müssen, um in die Gruppe eingeschlossen zu werden. ActiveRoles Server füllt die Mitgliedschaftsliste der Gruppe dynamisch mit den Objekten auf, die bestimmte Eigenschaften aufweisen. Wenn ein Objekt erstellt wird oder wenn seine Eigenschaften geändert werden, fügt ActiveRoles Server dieses Objekt der Gruppe hinzu bzw. entfernt es daraus, abhängig davon, ob die Eigenschaften des Objekts den definierten Kriterien entsprechen.

Mit der Mitgliedschaftsregel **Gruppenmitglieder einschließen** können Sie die Gruppen auswählen, deren Mitglieder Sie in die dynamische Gruppe einschließen möchten. ActiveRoles Server füllt die Mitgliedschaftsliste der Gruppe dynamisch mit den Objekten auf, die den ausgewählten Gruppen angehören. Wenn ein Objekt den ausgewählten Gruppen hinzugefügt oder aus ihnen entfernt wird, fügt ActiveRoles Server dieses Objekt der dynamischen Gruppe hinzu bzw. entfernt es aus ihr.

Mit der Mitgliedschaftsregel **Explizit ausschließen** können Sie Objekte auswählen, die aus der Gruppe statisch ausgeschlossen werden sollen. ActiveRoles Server stellt sicher, dass die ausgewählten Objekte auch dann aus der Mitgliedschaftsliste der Gruppe ausgeschlossen sind, wenn sie umbenannt oder verschoben werden oder wenn ihre Eigenschaften geändert werden. Da die Regel **Explizit ausschließen** Vorrang vor allen anderen Regeltypen hat, werden die ausgewählten Objekte auch dann aus der Gruppe ausgeschlossen, wenn eine andere Regel besagt, dass sie eingeschlossen werden sollen.

Mit der Mitgliedschaftsregel **Nach Abfrage ausschließen** können Sie Kriterien definieren, die die Objekte erfüllen müssen, um aus der Gruppe ausgeschlossen zu werden. ActiveRoles Server stellt sicher, dass Objekte mit bestimmten Eigenschaften aus der Mitgliedschaftsliste der Gruppe ausgeschlossen werden. ActiveRoles Server entfernt Objekte automatisch aus der Gruppe, abhängig davon, ob die Eigenschaften der Objekte den definierten Kriterien entsprechen.

Mit der Mitgliedschaftsregel **Gruppenmitglieder ausschließen** können Sie Gruppen auswählen, deren Mitglieder aus der jeweiligen Gruppe ausgeschlossen werden sollen. ActiveRoles Server stellt sicher, dass die Mitglieder der ausgewählten Gruppen aus der Mitgliedschaftsliste der Gruppe entfernt werden. Wenn ein Objekt einer der ausgewählten Gruppen hinzugefügt wird, entfernt ActiveRoles Server dieses Objekt automatisch aus der dynamischen Gruppe.

Wählen Sie auf der ersten Seite des Assistenten einen Regeltyp aus, und klicken Sie dann auf **Weiter**. Klicken Sie auf der nächsten Seite des Assistenten auf **Hinzufügen**, um die Mitgliedschaftsregel zu konfigurieren.

Wenn Sie den Regeltyp **Explizit einschließen** oder **Explizit ausschließen** ausgewählt, haben, wird das Dialogfeld **Objekte auswählen** angezeigt, in dem Benutzer, Gruppen, Kontakte und Computer aufgelistet werden. Wählen Sie die Objekte aus, die Sie in die dynamische Gruppe einschließen oder aus ihr ausschließen möchten, klicken Sie auf **Hinzufügen** und dann auf **OK**.

Wenn Sie den Regeltyp **Gruppenmitglieder einschließen** oder **Gruppenmitglieder ausschließen** ausgewählt haben, wird das Dialogfeld **Objekte auswählen** angezeigt. Die Liste der Objekte in diesem Dialogfeld besteht aus Gruppen. Wählen Sie Gruppen aus, klicken Sie auf **Hinzufügen** und dann auf **OK**. Alle Mitglieder der ausgewählten Gruppen werden in die dynamische Gruppe eingeschlossen oder aus ihr ausgeschlossen.

Wenn Sie den Regeltyp **Nach Abfrage einschließen** oder **Nach Abfrage ausschließen** ausgewählt haben, wird das Dialogfeld **Mitgliedschaftsregel erstellen** angezeigt, das dem Dialogfeld **Suchen** ähnelt. Definieren Sie in diesem Dialogfeld die Kriterien, die Objekte erfüllen müssen, um in die dynamische Gruppe eingeschlossen oder aus ihr ausgeschlossen zu werden.

Klicken Sie auf **Fertig stellen**, um den Assistenten „Neue Mitgliedschaftsregel" abzuschließen.

Nachdem Sie eine dynamische Gruppe erstellt und ihr dabei die erste Regel hinzugefügt haben, können Sie weitere Regeln hinzufügen. Verwenden Sie dazu die Verwaltungsfunktionen für Eigenschaften der Gruppe.

Wenn Sie mehrere Mitgliedschaftsregeln hinzufügen und einige davon miteinander in Konflikt stehen, wird der Konflikt durch eine Regel gelöst, die die folgende Rangordnung definiert:

1. Explizit ausschließen
2. Explizit einschließen
3. Nach Abfrage ausschließen
4. Gruppenmitglieder ausschließen
5. Nach Abfrage einschließen
6. Gruppenmitglieder einschließen

Nach dieser Rangfolge hat z.B. die Regel **Explizit ausschließen** Vorrang vor allen anderen Regeltypen. Daher werden die ausgewählten Objekte auch dann aus der dynamischen Gruppe ausgeschlossen, wenn eine andere Regel angibt, dass sie eingeschlossen werden sollen (beispielsweise die Objekte, die die in der Mitgliedschaftsregel **Nach Abfrage einschließen** definierten Kriterien erfüllen, oder Mitglieder eine Gruppe, die in der Regel **Gruppenmitglieder einschließen** ausgewählt wurden).

Anzeigen der Mitglieder einer dynamischen Gruppe

Für eine dynamische Gruppe wird dem Dialogfeld **Eigenschaften** die Registerkarte **Mitgliedschafts-regeln** hinzugefügt. Auf dieser Registerkarte wird eine Liste von Mitgliedschaftsregeln angezeigt, die für die Gruppe definiert sind. Außerdem können Sie hier die Regeln hinzufügen, entfernen und bearbeiten.

Auf der Registerkarte **Mitglieder** für eine dynamische Gruppe wird eine Liste von Objekten angezeigt, die den in den Mitgliedschaftsregeln angegebenen Kriterien entsprechen. Auf dieser Registerkarte können Sie Mitglieder nicht wie bei einer Standardgruppe hinzufügen oder entfernen. Um bestimmte Mitglieder einer dynamischen Gruppe hinzuzufügen oder zu entfernen, können Sie eine entsprechende Mitgliedschaftsregel der Art **Explizit einschließen** oder **Explizit ausschließen** hinzufügen.

Hinzufügen einer Mitgliedschaftsregel zu einer dynamischen Gruppe

Um eine Mitgliedschaftsregel zu einer dynamischen Gruppe hinzuzufügen, klicken Sie mit der rechten Maustaste auf die dynamische Gruppe, und klicken Sie dann auf **Mitgliedschaftsregel hinzufügen**. Hierdurch wird der Assistent „Neue Mitgliedschaftsregel" gestartet. Schließen Sie den Assistenten wie unter „Konvertieren einer Standardgruppe in eine dynamische Gruppe" weiter oben in diesem Kapitel beschrieben ab.

Um einer dynamischen Gruppe eine Mitgliedschaftsregel hinzuzufügen, können Sie auch die Registerkarte **Mitgliedschaftsregeln** im Dialogfeld **Eigenschaften** verwenden. Schrittweise Anleitungen bezüglich des Hinzufügens von Mitgliedschaftsregeln zu dynamischen Gruppen finden Sie unter **Anleitungen/Verwalten von Gruppen/Hinzufügen einer Mitgliedschaftsregel zu einer Gruppe** in der ActiveRoles Server-Hilfe.

Entfernen einer Mitgliedschaftsregel aus einer dynamischen Gruppe

Um eine Mitgliedschaftsregel aus einer dynamischen Gruppe zu entfernen, öffnen Sie das Dialogfeld **Eigenschaften** für die Gruppe. Wählen Sie auf der Registerkarte **Mitgliedschaftsregeln** die zu entfernenden Mitgliedschaftsregeln aus, und klicken Sie dann auf **Entfernen**. Klicken Sie danach auf **OK**, um das Dialogfeld **Eigenschaften** zu schließen.

In ActiveRoles Server können Mitglieder nicht durch direkte Verwaltung der Mitgliedschaftsliste der Gruppe aus einer dynamischen Gruppe entfernt werden. Um bestimmte Mitglieder zu entfernen, können Sie Regeln der Art **Explizit ausschließen** konfigurieren.

Schrittweise Anleitungen bezüglich des Entfernens von Mitgliedschaftsregeln aus dynamischen Gruppen finden Sie unter **Anleitungen/Verwalten von Gruppen/Entfernen einer Mitgliedschaftsregel aus einer Gruppe** in der ActiveRoles Server-Hilfe.

Konvertieren einer dynamischen Gruppe in eine Standardgruppe

Beim Konvertieren einer dynamischen Gruppe in eine Standardgruppe werden nur die Mitgliedschaftsregeln aus der Gruppe entfernt. Die Mitgliedschaftsliste der Gruppe bleibt unverändert. Klicken Sie zum Konvertieren einer dynamischen Gruppe in eine Standardgruppe mit der rechten Maustaste auf die Gruppe, und klicken Sie dann auf **In Standardgruppe konvertieren**. Klicken Sie im Bestätigungsfeld auf **Ja**.

Wenn eine Gruppe nicht mehr dynamisch ist, wird sie zu einer Standardgruppe mit den folgenden Eigenschaften:

- Im Dialogfeld **Eigenschaften** wird die Registerkarte **Mitgliedschaftsregeln** nicht mehr angezeigt.
- Auf der Registerkarte **Mitglieder** können Sie Mitglieder hinzufügen und entfernen (die Schaltflächen **Hinzufügen** und **Entfernen** werden auf der Registerkarte **Mitglieder** angezeigt).

Ändern, Löschen und Umbenennen einer dynamischen Gruppe

Sie können dynamische Gruppen auf die gleiche Weise verwalten wie Standardgruppen (reguläre Gruppen): Sie können sie umbenennen, Eigenschaften ändern, ihnen beim Delegieren der Kontrolle einen Trustee zuweisen sowie sie löschen. Die Anweisungen zur Ausführung solcher Verwaltungsaufgaben für dynamische Gruppen sind die gleichen wie bei regulären Gruppen. Schrittweise Anleitungen bezüglich der Verwaltung von Gruppen finden Sie unter **Anleitungen/Verwalten von Gruppen** in der ActiveRoles Server-Hilfe.

Szenario: Automatisches Verschieben von Benutzern zwischen Gruppen

In diesem Szenario wird ein Benutzer aufgrund eines Umzugs von Seattle nach Atlanta aus der Gruppe **Seattle** entfernt und der Gruppe **Atlanta** hinzugefügt.

Angenommen, die Benutzerkonten von Mitarbeitern in Seattle gehören der Gruppe **Seattle** an, und Benutzerkonten von Mitarbeitern in Atlanta gehören der Gruppe **Atlanta** an. Die Gruppe, zu der ein Benutzer gehört, wird durch das Stadtattribut definiert: Bei Mitarbeitern in Seattle hat das Attribut **Stadt** des Benutzerkontos den Wert „Seattle". Bei Mitarbeitern in Atlanta lautet dieser Wert „Atlanta".

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen Sie die Gruppen für Seattle und Atlanta.
2. Konfigurieren Sie Mitgliedschaftsregeln, um Benutzer diesen beiden Gruppen zuzuordnen.

Daraufhin gehören nur Benutzerkonten, deren Stadtattributwert „Seattle" lautet, der Gruppe „Seattle" an. Wenn ein Mitarbeiter von Seattle nach Atlanta versetzt wird, ändert ein Administrator das Attribut **Stadt** entsprechend, und der Benutzer wird aufgrund der Mitgliedschaftsregel automatisch in die Gruppe **Atlanta** verschoben. Wenn ein Mitarbeiter von Atlanta nach Seattle versetzt wird, ändert ebenfalls ein Administrator das Stadtattribut, und der Benutzer wird automatisch in die Gruppe **Seattle** übertragen.

In den folgenden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen der Gruppen

Um die Gruppe **Seattle** zu erstellen, klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf den Container, zu dem Sie die Gruppe hinzufügen möchten, und wählen Sie dann **Neu | Gruppe**. Befolgen Sie die Anweisungen des Assistenten unter „Neues Objekt – Gruppe". Geben Sie in das Feld **Gruppenname** den Wert **Seattle** ein.

Um die Gruppe **Atlanta** zu erstellen, klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf den Container, zu dem Sie die Gruppe hinzufügen möchten, und wählen Sie dann **Neu | Gruppe**. Befolgen Sie die Anweisungen des Assistenten unter „Neues Objekt – Gruppe". Geben Sie in das Feld **Gruppenname** den Wert **Atlanta** ein.

Schrittweise Anleitungen bezüglich der Erstellung von Gruppen finden Sie unter **Anleitungen/Verwalten von Gruppen/Erstellen einer Gruppe** in der ActiveRoles Server-Hilfe.

Schritt 2: Konfigurieren der Mitgliedschaftsregeln

In diesem Szenario hat bei Mitarbeitern in Seattle das Attribut **Stadt** des Benutzerkontos den Wert „Seattle". Bei den Mitarbeitern in Atlanta hat es den Wert „Atlanta".

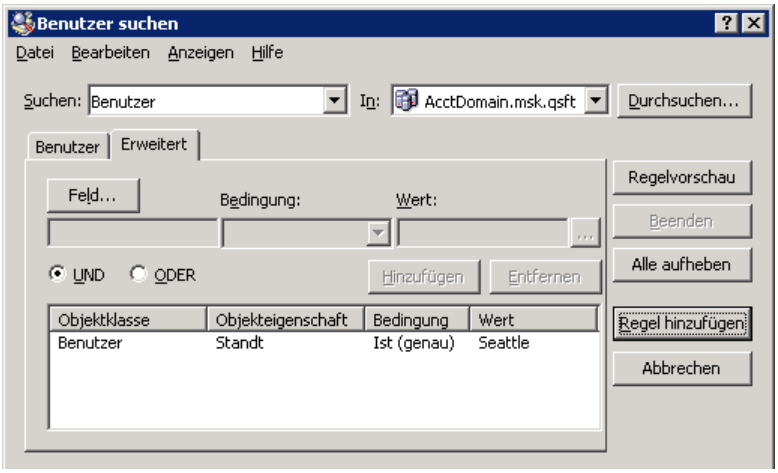
Konfigurieren Sie zuerst die Mitgliedschaftsregel für die Gruppe **Seattle**. Klicken Sie mit der rechten Maustaste auf die Gruppe, und klicken Sie dann auf **In dynamische Gruppe konvertieren**. Klicken Sie im Bestätigungsfeld auf **Ja**.

Klicken Sie auf der ersten Seite des Assistenten „Neue Mitgliedschaftsregel" auf **Nach Abfrage einschließen** und klicken Sie dann auf **Weiter**.

Klicken Sie auf der zweiten Seite auf **Hinzufügen**, um das Dialogfeld **Mitgliedschaftsregeln erstellen** anzuzeigen. Konfigurieren Sie dann die Mitgliedschaftsregel anhand der folgenden Schritte:

1. Klicken Sie in der Liste **Suchen** auf **Benutzer**.
2. Klicken Sie auf **Durchsuchen** und wählen Sie die Domäne, Organisationseinheit oder verwaltete Einheit aus, die Benutzerkonten der Mitarbeiter enthält.
3. Klicken Sie auf die Registerkarte **Erweitert**.
4. Klicken Sie auf **Feld**, zeigen Sie auf **Benutzer**, und klicken Sie dann auf **Stadt**.
5. Klicken Sie in der Liste **Bedingung** auf **Ist (genau)**.
6. Geben Sie in das Feld **Wert** den Wert **Seattle** ein.
7. Klicken Sie auf **Hinzufügen**.

Nach der Ausführung dieser Schritte entspricht das Dialogfeld der folgenden Abbildung.



Klicken Sie auf die Schaltfläche **Regel hinzufügen**. Klicken Sie dann im Assistenten „Neue Mitgliedschaftsregel" auf **Fertig stellen**, um den Vorgang abzuschließen.

Jetzt ist die Gruppe **Seattle** so konfiguriert, dass sie die Benutzerkonten einschließt, deren Attribut **Stadt** den Wert „Seattle" aufweist.

Wiederholen Sie den gleichen Vorgang für die Gruppe **Atlanta**, aber geben Sie beim Konfigurieren der Mitgliedschaftsregel in das Feld **Wert** den Wert **Atlanta** ein.

11

ActiveRoles Server-Berichterstattung

- Einleitung
- Datenvorbereitungs-Collector für Berichte
- Quest Knowledge Portal für die Anzeige von Berichten
- Arbeiten mit Berichten

Einleitung

Die ActiveRoles Server-Berichterstattungslösung macht Microsoft SQL Server Reporting Services (SSRS) zu einer Plattform für die Verwaltung, Erzeugung und Anzeige von Berichten.

Durch die Nutzung von SSRS bietet ActiveRoles Server Berichterstattungsfunktionen der Unternehmensklasse, die die Vorteile von webbasierten Funktionen mit der herkömmlichen Berichterstattung kombinieren. Die Verwendung von Reporting Services bietet die Möglichkeit zur Zentralisierung der Berichtsspeicherung und -verwaltung, einen sicheren Zugriff auf Berichte, die Kontrolle über die Verarbeitung und Verbreitung der Berichte sowie Standards bezüglich der Verwendung der Berichte.

Eine umfassende Sammlung von Berichtsdefinitionen, die als das *ActiveRoles Server Report Pack* bezeichnet werden, werden auf dem Berichtsserver, einer Komponente von Reporting Services, veröffentlicht. Durch die Installation von Report Pack werden veröffentlichte Berichte erstellt, auf die über Webadressen (URLs), über SharePoint Web-Komponenten oder über Report Manager, ein im Lieferumfang von SSRS enthaltenes, webbasiertes Berichtszugriffs- und -verwaltungstool, zugegriffen werden kann.

Eine weitere Option für den Zugriff auf veröffentlichte Berichte ist das Quest Knowledge Portal, eine webbasierte Anwendung, die die Funktionen von SSRS erweitern, um eine einfache Berichtsverwaltung und -bereitstellung zu ermöglichen. Mit Quest Knowledge Portal kann ein Administrator schnell und einfach Berichte in einer Ordnerhierarchie organisieren, Datenquellen konfigurieren, Berichtseigenschaften ändern, Berichte exportieren und importieren und die Berichte durchsuchen.

Durch Öffnen eines veröffentlichten Berichts vom Berichtsserver wird der Bericht in einem für die Anzeige geeigneten Format generiert. Diese Aktion wird *Generierung eines Berichts* genannt. Die Generierung eines Berichts erfolgt auch bei einem Abonnement, wenn der Bericht an ein E-Mail-Eingangsfach oder an eine Dateifreigabe in einem vom Berichtsbenutzer angegebenen Ausgabeformat gesendet wird.

Standardmäßig generiert der Berichtsserver die Berichte im HTML-Format. Zusätzlich zu HTML können die Berichte in einer Vielzahl von Ausgabeformaten einschließlich Excel, XML, PDF, TIFF und CSV generiert werden. Berichtsbenutzer können wählen, ob die Berichte auf Anforderung in einem bevorzugten Format für die Datenbearbeitung generiert oder ausgedruckt werden.

Die Berichte, die generiert werden können, sobald ActiveRoles Server Report Pack installiert ist, sind ganz entscheidend für Überprüfung und Verfolgung von Änderungen, für die Überwachung und Analyse von Verzeichnisdaten und für die Bewertung der ActiveRoles Server Sicherheits- und Richtlinienkonfigurationen. Die Berichte lassen sich in die folgenden Kategorien einteilen:

- **ActiveRoles Server-Verlaufsprotokoll** Überprüfen Sie, welche Änderungen mit Hilfe von ActiveRoles an den Verzeichnisdaten vorgenommen wurden, wer diese Änderungen vorgenommen hat und wann diese Änderungen erfolgt sind.
- **Active Directory-Bewertung** Untersuchen Sie den Status von Verzeichnisdaten wie etwa die Eigenschaften von Benutzern, Gruppen und anderen Verzeichnisobjekten, Gruppenmitgliedschaftslisten und die Inhalte von Organisationseinheiten.
- **Administratorfunktionen** Zeigen Sie Details darüber an, wer bei Verwendung von ActiveRoles Server Zugriff auf welche Daten hat und welche Änderungen administrative Benutzer oder Gruppen vornehmen dürfen.

- **Verwaltete Einheiten** Zeigen Sie Details zu den in der ActiveRoles Server-Umgebung definierten verwalteten Einheiten, welche Richtlinien auf die verwalteten Einheiten angewandt sind und welche Benutzer oder Gruppen über einen administrativen Zugriff auf welche verwalteten Einheiten haben an.
- **Richtlinienobjekte** Zeigen Sie Details dazu an, welche administrative Richtlinien in der ActiveRoles Server-Umgebung definiert sind, wo bestimmte Richtlinien angewandt werden und welche Richtlinien für bestimmte Objekte und Container in Kraft sind.
- **Richtlinienkonformität** Zeigen Sie Details darüber an, welche Daten im Verzeichnis nicht mit den gültigen ActiveRoles Server-Richtlinien konform sind und gegen welche Richtlinienregeln verstoßen wurde.

Berichte werden auf der Grundlage der vom ActiveRoles Server Collector vorbereiteten Daten erstellt. Nähere Informationen zum ActiveRoles Server Collector finden Sie unter „Collector für die Vorbereitung der Berichtsdaten" weiter unten in diesem Kapitel.

Sie können Berichte mit Hilfe von Report Manager, einem Bestandteil von SSRS, generieren und anzeigen. Eine weitere Möglichkeit, Berichte zu generieren und anzuzeigen, ist die Nutzung von Quest Knowledge Portal, einem webbasierten Berichtsmanagementtool von Quest Software. Quest Knowledge Portal bietet eine einfache und bequeme Möglichkeit für die Generierung und Anzeige von Berichten, die auf vom ActiveRoles Server Collector erfassten Daten beruhen. Nähere Informationen über das Quest Knowledge Portal finden Sie unter „Quest Knowledge Portal für die Anzeige von Berichten" weiter unten in diesem Kapitel. Weitere Informationen über das Quest Knowledge Portal finden Sie in der diesem Produkt beiliegenden Dokumentation.

Anweisungen bezüglich der Generierung und Anzeige von Berichten finden Sie unter „Arbeiten mit Berichten" weiter unten in diesem Kapitel.

Datenvorbereitungs-Collector für Berichte

Mit dem Collector von ActiveRoles Server können Sie Daten von Computern sammeln, auf denen der Verwaltungsdienst ausgeführt wird, und diese Daten in einer SQL Server-Datenbank speichern, sodass die Daten für die Berichterstattung verfügbar werden.

Der ActiveRoles Server Collector wird als eine separate Komponente von ActiveRoles Server installiert.

Daten für Berichte werden aus den folgenden Quellen gesammelt:

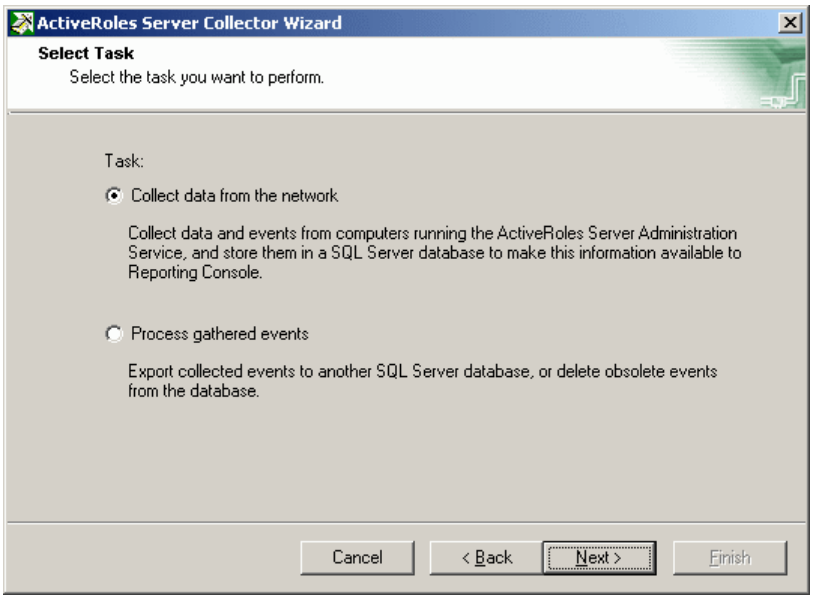
- **Active Directory** Der Collector greift auf Active Directory über den Verwaltungsdienst zu. Berichte, die auf diesen Daten basieren, enthalten detaillierte Informationen zu Domänen, Konten, Gruppen und anderen Active Directory-Objekten.
- **ActiveRoles Server-Konfigurationsdatenbank** Berichte, die auf diesen Daten basieren, enthalten detaillierte Informationen dazu, wer mit ActiveRoles Server welche Aktionen für welche Verzeichnisobjekte ausführen kann. Außerdem enthalten sie Informationen zu den von ActiveRoles Server definierten Richtlinien.
- **Ereignisprotokoll auf Computern, die den Verwaltungsdienst ausführen** Berichte, die auf diesen Daten basieren, enthalten detaillierte Informationen zu ausgeführten Aktionen, zum Erfolg oder Fehler jeder Aktion sowie zu Objekteigenschaften, die mit ActiveRoles Server geändert wurden.

Der Bereich der Daten, die der Collector aus Active Directory abrufen kann, wird durch die Zugriffsrechte des Benutzerkontos beschränkt, mit dem der Collector die Datenerfassungsaufgabe ausführt. Daher können Berichte, die auf Active Directory-Daten basieren, nur Informationen zu den Objekten enthalten, auf die der Collector in Active Directory zugreifen darf.

Nehmen Sie beispielsweise an, dass der Collector eine Datenerfassungsaufgabe mit dem Benutzerkonto ausführt, das nicht über Zugriffsrechte für Benutzerkontoeigenschaften in Active Directory verfügt. Dann kann der Collector keine Daten zu Benutzerkonten abrufen, und in den Berichten sind keine Informationen zu Benutzerkonten enthalten, auch nicht die Anzahl der Benutzerkonten.

Um Daten für Berichte zu sammeln, starten Sie den Assistenten „ActiveRoles Server Collector": Klicken Sie auf **Starten** und wählen Sie dann **Alle Programme | Quest Software | ActiveRoles Server | Collector**. Klicken Sie dann im Assistenten auf **Next (Weiter)**, um die Seite **Select Task (Aufgabe auswählen)** anzuzeigen, die in der folgenden Abbildung dargestellt ist.

Sie können auf jeder Seite des Assistenten auf Informationen zu der Seite zugreifen, indem Sie die F1-Taste drücken.

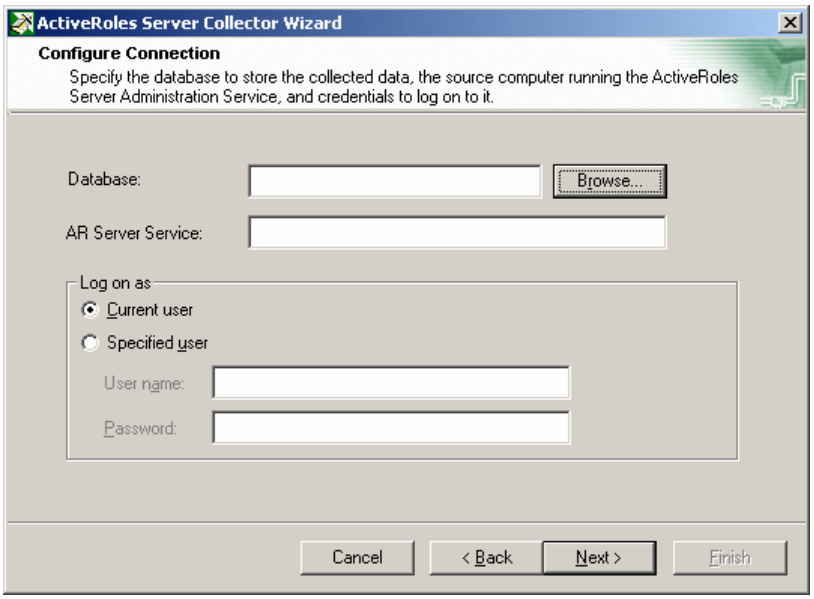

ActiveRoles Server Collector Wizard
Select Task
Select the task you want to perform.
Task:
Collect data from the network
Collect data and events from computers running the ActiveRoles Server Administration Service, and store them in a SQL Server database to make this information available to Reporting Console.
Process gathered events
Export collected events to another SQL Server database, or delete obsolete events from the database.
Cancel
< Back
Next >
Finish

Auf dieser Seite können Sie eine der folgenden Aufgaben für die Ausführung auswählen:

- **Collect data from the network (Daten aus dem Netzwerk erfassen)** Sammelt Daten und Ereignisse von den Computern, auf denen der Verwaltungsdienst ausgeführt wird, und speichert die gesammelten Information in einer SQL Server-Datenbank, um die Informationen für den Berichtsserver verfügbar zu machen.
- **Process gathered events (Gesammelte Ereignisse verarbeiten)** Exportiert ausgewählte Ereignisse in eine andere SQL Server-Datenbank oder löscht veraltete Informationen aus der Datenbank.

Sammeln von Daten aus dem Netzwerk

Wenn Sie auf der Seite **Select Task (Aufgabe auswählen)** die Option **Collect data from the network (Daten aus dem Netzwerk erfassen)** auswählen, zeigt der Assistent im nächsten Schritt die Seite **Configure Connection (Verbindung konfigurieren)** an.



Auf der Seite **Configure Connection (Verbindung konfigurieren)** des Assistenten werden Sie aufgefordert, die anfänglichen Optionen für die Verwaltung der Daten anzugeben: Datenbank, in der die erfassten Daten gespeichert werden sollen; Quellcomputer, auf dem der Verwaltungsdienst ausgeführt wird; und die Anmeldeinformationen für die Anmeldung bei diesem Computer.

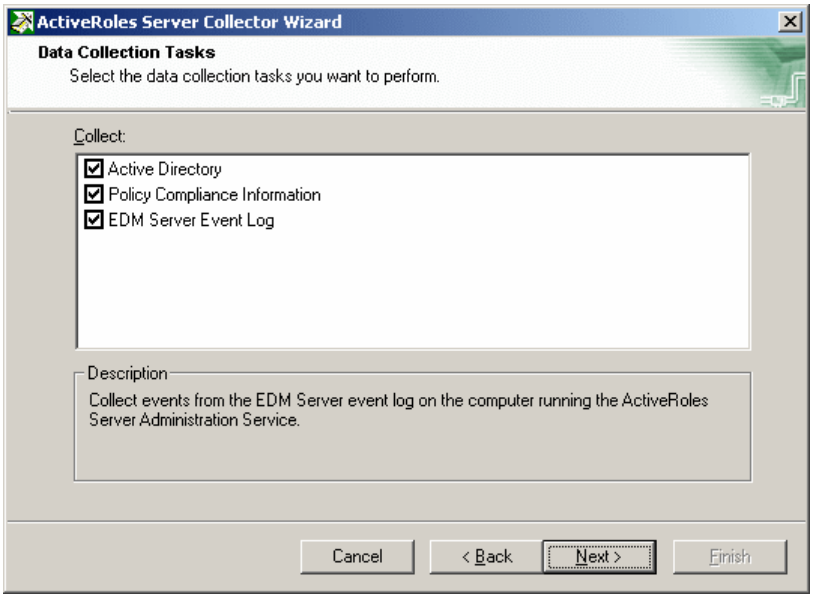
Um eine Datenbank anzugeben oder eine andere Datenbank auszuwählen, klicken Sie auf **Browse (Durchsuchen)**. Damit können Sie auf den Assistenten „SQL Server-Verbindung" zugreifen, der Sie durch den Konfigurationsvorgang für die Verbindung mit der Datenbank führt.

Geben Sie im Feld **AR Server Service (AR Server-Dienst)** den vollständigen Namen des Computers mit dem Verwaltungsdienst an, von dem Sie Informationen sammeln möchten.

Geben Sie im Bereich **Log on as (Anmelden als)** die Rechtezuweisungen an, mit denen der Collector sich beim Verwaltungsdienst anmelden soll. Sie können eine der folgenden Optionen auswählen:

- **Current user (Aktueller Benutzer)** Stellt die Verbindung zum Verwaltungsdienst mit den Rechtezuweisungen des Benutzerkontos her, mit dem der Collector gestartet wird.
- **Specified user (Angegebener Benutzer)** Stellt die Verbindung zum Verwaltungsdienst mit den angegebenen Rechtezuweisungen her (Benutzername und Kennwort).

Klicken Sie auf **Next (Weiter)**, um mit der Seite **Data Collection Tasks (Datenerfassungsaufgaben)** fortzufahren.

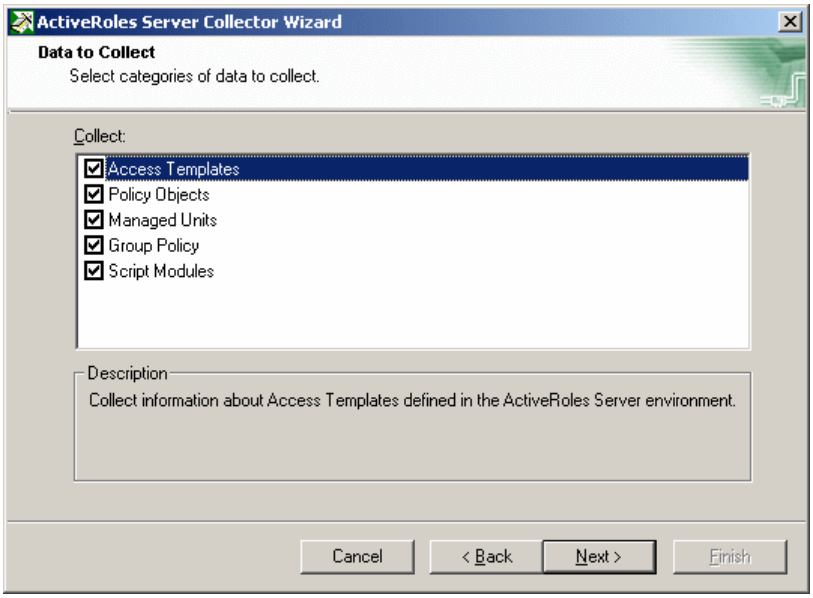

ActiveRoles Server Collector Wizard
Data Collection Tasks
Select the data collection tasks you want to perform.
Collect:
Active Directory
Policy Compliance Information
EDM Server Event Log
Description
Collect events from the EDM Server event log on the computer running the ActiveRoles Server Administration Service.
Cancel
< Back
Next >
Finish

Auf der Seite **Data Collection Tasks (Datenerfassungsaufgaben)** des Assistenten werden Sie aufgefordert, die Quellen der zu sammelnden Daten anzugeben. Sie können folgende Quellen auswählen:

- **Active Directory** Informationen zu Benutzern, Gruppen, Computern, Organisationseinheiten und Domänen von Active Directory.
- **Policy Compliance Information (Richtlinienkonformitätsinformationen)** Informationen darüber, ob die Active Directory-Daten mit den von ActiveRoles Server definierten Richtlinien konform sind oder nicht. Erfordert, dass Daten auch von Active Directory erfasst werden (das Kontrollkästchen **Active Directory** muss aktiviert sein).
- **EDM Server Event Log (EDM Server-Ereignisprotokoll)** Informationen aus dem **EDM-Server**-Ereignisprotokoll auf dem Computer, auf dem der Verwaltungsdienst ausgeführt wird.

Klicken Sie auf **Next (Weiter)**, um mit der Seite **Data to Collect (Zu erfassende Daten)** fortzufahren.

Der Assistent zeigt die Seite **Data to Collect (Zu erfassende Daten)** nur an, wenn Sie auf der Seite **Data Collection Tasks (Datenerfassungsaufgaben)** das Kontrollkästchen **Active Directory** aktivieren.

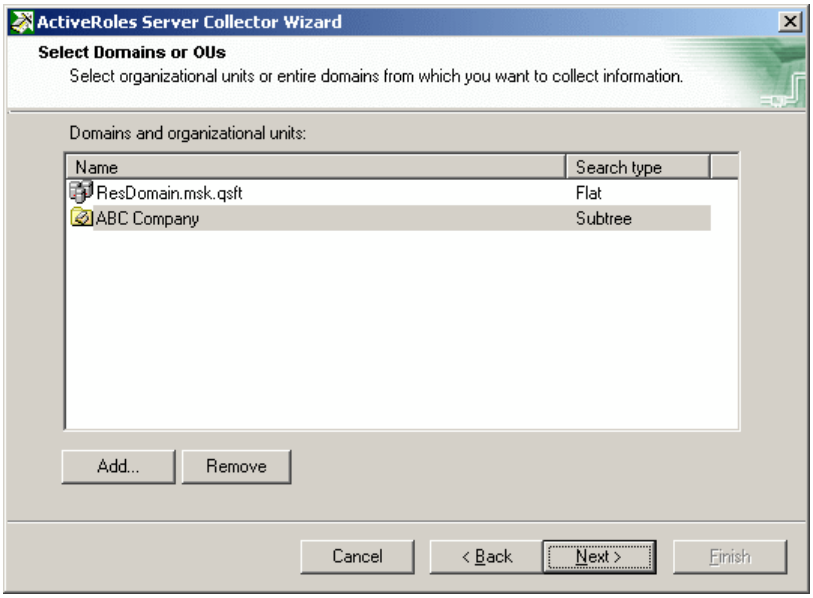


Auf der Seite **Data to Collect (Zu erfassende Daten)** des Assistenten werden Sie aufgefordert, die Kategorien der zu sammelnden Daten anzugeben. Sie können folgende Kategorien auswählen:

- **Access Templates (Zugriffsvorlagen)** Informationen zu Zugriffsvorlagen, die in der ActiveRoles Server-Umgebung definiert sind.
- **Policy Objects (Richtlinienobjekte)** Informationen zu Richtlinienobjekten, die in der ActiveRoles Server-Umgebung definiert sind.
- **Managed Units (Verwaltete Einheiten)** Informationen zu verwalteten Einheiten, die in der ActiveRoles Server-Umgebung definiert sind.
- **Group Policy (Gruppenrichtlinie)** Gruppenrichtlinienbezogene Informationen.
- **Script Modules (Skriptmodule)** Informationen zu Skriptmodulen, die in der ActiveRoles Server-Umgebung definiert sind.

Wenn Sie auf der vorigen Seite das Kontrollkästchen **Policy Compliance Information (Richtlinienkonformitätsinformationen)** aktiviert haben, können Sie auf der Seite **Data to Collect (Zu erfassende Daten)** das Kontrollkästchen **Policy Objects (Richtlinienobjekte)** nicht deaktivieren.

Klicken Sie auf **Next (Weiter)**, um mit der Seite **Select Domains or OUs (Domänen oder Organisationseinheiten auswählen)** fortzufahren.

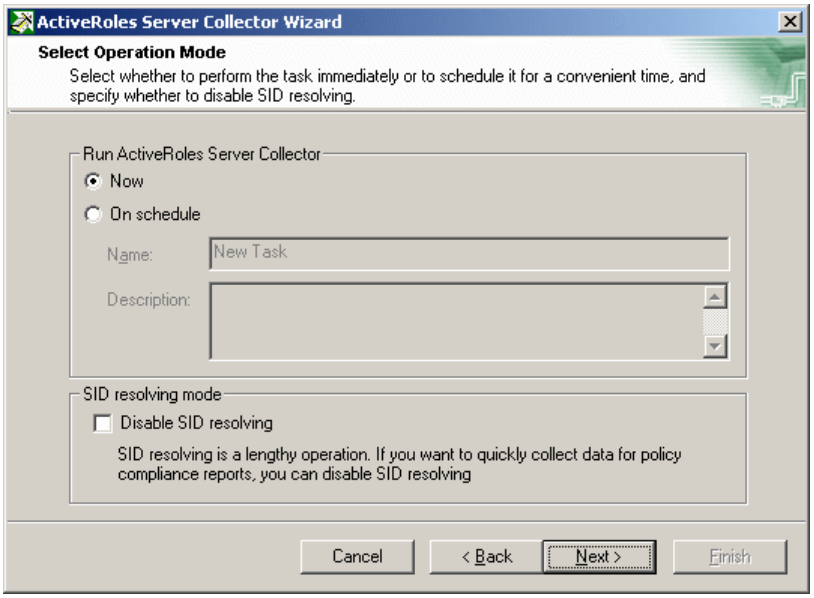


Auf der Seite **Select Domains or OUs (Domänen oder Organisationseinheiten auswählen)** des Assistenten werden Sie aufgefordert, die Domänen oder Container anzugeben, aus denen Sie Informationen sammeln möchten. Sie können diese Seite wie folgt ausfüllen:

- Klicken Sie auf **Add (Hinzufügen)**, um der Liste auf der Seite eine Domäne oder Organisationseinheit hinzuzufügen.
- Klicken Sie auf **Remove (Entfernen)**, um eine ausgewählte Domäne oder Organisationseinheit aus der Liste zu löschen.

Wenn Sie eine Domäne oder Organisationseinheit auswählen, können Sie wie folgt erzwingen, dass der Assistent Informationen über alle untergeordneten Objekte der ausgewählten Domäne oder Organisationseinheit erfassen soll: Aktivieren Sie in dem Dialogfeld, das durch Klicken auf **Add (Hinzufügen)** angezeigt wird, das Kontrollkästchen **Use subtree search (Teilstruktursuche verwenden)**. Wenn Sie das Kontrollkästchen **Use subtree search (Teilstruktursuche verwenden)** deaktivieren, erfasst der Assistent nur Informationen über die unmittelbaren untergeordneten Objekte der ausgewählten Domäne oder Organisationseinheit.

Klicken Sie auf **Next (Weiter)**, um mit der Seite **Select Operation Mode (Betriebsart auswählen)** fortzufahren.


ActiveRoles Server Collector Wizard
Select Operation Mode
Select whether to perform the task immediately or to schedule it for a convenient time, and specify whether to disable SID resolving.
Run ActiveRoles Server Collector
Now
On schedule
Name:
New Task
Description:
SID resolving mode
Disable SID resolving
SID resolving is a lengthy operation. If you want to quickly collect data for policy compliance reports, you can disable SID resolving
Cancel
< Back
Next >
Finish

Auf der Seite **Select Operation Mode (Betriebsart auswählen)** können Sie angeben, dass die Taskausführung sofort gestartet werden soll, oder Sie können sie für einen passenden Zeitpunkt planen. Sie können auch die SID-Auflösung deaktivieren, damit Daten schneller gesammelt werden.

Wenn Sie den Sammlungsprozess sofort starten möchten, wählen Sie unter **Run ActiveRoles Server Collector (ActiveRoles Server Collector ausführen)** die Option **Now (Jetzt)** aus, und klicken Sie auf **Next (Weiter)**. Während der Assistent den Vorgang ausführt, wird der Statusbildschirm angezeigt, in dem der Fortschritt detailliert zu erkennen ist.

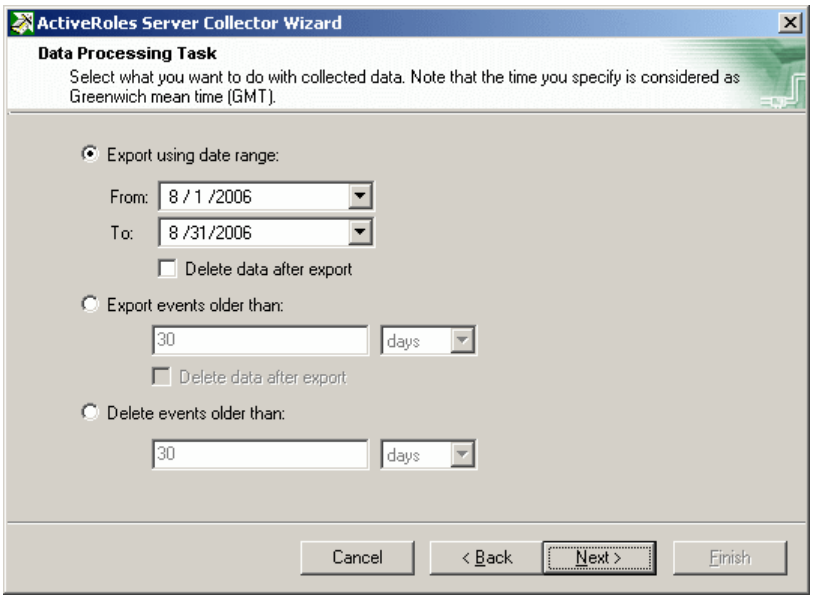
Nach Abschluss des Vorgangs wird das Abschlussfenster des Assistenten mit den Vorgangsergebnissen angezeigt. Sie können auf **View Log (Protokoll anzeigen)** klicken, um das Vorgangsprotokoll auf etwaige Fehler zu untersuchen.

Wenn Sie für den Task einen Zeitplan festlegen möchten, wählen Sie **On schedule (Nach Zeitplan)** aus, und klicken Sie auf **Next (Weiter).** Dann wird die Seite **Schedule (Zeitplan)** angezeigt, auf der Sie den Zeitplan und das Anmeldekonto für den Task angeben können. Klicken Sie auf **Change (Ändern)**, um einen Zeitplan für den Task zu erstellen. Klicken Sie auf **Account (Konto)**, um den Benutzernamen und das Kennwort des Benutzerkontos anzugeben, mit dem der Task ausgeführt werden soll. Wenn Sie die Zeitplanoptionen festgelegt haben, klicken Sie auf **Next (Weiter)**, um den Assistenten abzuschließen.

Schrittweise Anleitungen bezüglich der Erfassung von Daten mit Hilfe von ActiveRoles Server Collector finden Sie unter **Anleitungen/Arbeiten mit Berichten/Erfassen von Daten** in der ActiveRoles Server-Hilfe.

Verarbeiten gesammelter Ereignisse

Wenn Sie auf der Seite **Select Task (Aufgabe auswählen)** die Option **Process gathered events (Gesammelte Ereignisse verarbeiten)** auswählen, zeigt der Assistent im nächsten Schritt die Seite **Data Processing Task (Datenverarbeitungsaufgabe)** an.



Auf dieser Seite des Assistenten geben Sie an, was mit den Ereignissen geschehen soll, die von Verwaltungsdienstcomputern gesammelt und in der Datenbank gespeichert wurden. Sie können eine der folgenden Optionen auswählen:

- **Export using date range (Exportieren mit Hilfe des Datenbereichs)** Geben Sie den Datumsbereich für die zu exportierenden Ereignisse an. Die Zeitpunkte, die Sie angeben, werden als Greenwich Mean Time (GMT) interpretiert.
- **Export events older than (Ereignisse älter als... exportieren)** Geben Sie die Altersgrenze für die zu exportierenden Ereignisse an.
- **Delete events older than (Ereignisse älter als... löschen)** Geben Sie die Altersgrenze für die zu löschenden Ereignisse an.

Klicken Sie auf **Next (Weiter)**, um die Seite **Source Database (Quelldatenbank)** anzuzeigen. Auf dieser Seite können Sie die Datenbank auswählen, aus der Sie Informationen exportieren oder löschen möchten. Außerdem können Sie hier die Anmeldeeinstellung für die Verbindung mit SQL Server festlegen. Um eine Datenbank auszuwählen, klicken Sie auf **Browse (Durchsuchen)**. Damit können Sie auf den Assistenten „SQL Server-Verbindung" zugreifen, der Sie durch den Konfigurationsvorgang für die Verbindung mit der Datenbank führt.

Klicken Sie auf **Next (Weiter)**, um den Vorgang fortzusetzen.

Wenn Sie die Exportoption für Informationen ausgewählt haben, zeigt der Assistent die Seite **Target Database (Zieldatenbank)** an. Diese ähnelt der Seite **Source Database (Quelldatenbank)**. Auf der Seite für die Zieldatenbank können Sie die Datenbank auswählen, in die Sie Informationen exportieren möchten. Außerdem können Sie hier die Anmeldeeinstellung für die Verbindung mit SQL Server festlegen. Um eine Datenbank auszuwählen, klicken Sie auf **Browse (Durchsuchen)**. Damit können Sie auf den Assistenten „SQL Server-Verbindung" zugreifen, der Sie durch den Konfigurationsvorgang für die Verbindung mit der Datenbank führt. Klicken Sie danach auf **Next (Weiter)**, um den Vorgang zu starten.

Während der Assistent den ausgewählten Vorgang ausführt, wird der Statusbildschirm angezeigt, in dem der Fortschritt detailliert zu erkennen ist.

Nach Abschluss des Vorgangs wird das Abschlussfenster des Assistenten mit den Vorgangsergebnissen angezeigt. Sie können auf **View Log (Protokoll anzeigen)** klicken, um das Vorgangsprotokoll auf etwaige Fehler zu untersuchen.

Quest Knowledge Portal für die Anzeige von Berichten

Quest Knowledge Portal ist ein webbasiertes Berichterstattungstool, das Microsoft SQL Server Reporting Services (SSRS) um zusätzliche Optionen erweitert, um eine einfache Berichtsverwaltung und -bereitstellung zu ermöglichen. Mit Quest Knowledge Portal können Sie folgende Aktionen ausführen:

- Anzeigen von Berichten über vom ActiveRoles Server Collector vorbereitete Daten
- Abonnieren der Berichte
- Durchsuchen der Berichte nach den von Ihnen benötigten Informationen
- Starten von Report Builder zur Erstellung von benutzerdefinierten Berichten
- Erstellen einer hierarchischen Struktur für die Berichtsordner
- Anzeigen oder Ändern der Eigenschaftseinstellungen für Berichte und Ordner

Anweisungen bezüglich der Installation und der Verwendung dieses Tools finden Sie in der im Lieferumfang von Quest Knowledge Portal enthaltenen Dokumentation. Dieser Abschnitt enthält eine kurze Übersicht über einige grundlegende Optionen von Quest Knowledge Portal.

Verwalten von Berichten und Ordnern

Um Berichte und Berichtsordner in Quest Knowledge Portal zu verwalten, klicken Sie auf die Registerkarte **Berichte** im linken Bereich des Quest Knowledge Portal-Fensters.

Klicken Sie anschließend durch die Berichtsordner, um den gewünschten Bericht zu suchen, und klicken Sie dann auf den Namen des Berichts. Sie können die folgenden Optionen auswählen:

- **Bericht anzeigen** Öffnen Sie die Berichtsanzeigeseite, auf der Sie Berichtsparameter festlegen und den Bericht generieren und anzeigen können.
- **Bericht in einem neuen Fenster anzeigen** Öffnen Sie die Berichtsanzeigeseite in einem separaten Fenster.
- **Sicherheitseinstellungen** Kontrollieren Sie den Benutzerzugriff auf den Bericht, indem Sie Benutzern oder Gruppen die entsprechenden Rollen in SSRS zuweisen.
- **Berichtseigenschaften** Zeigen Sie die Eigenschaften des Berichts an oder ändern Sie diese.

- **Berichtsansicht anpassen** Ändern Sie die Art und Weise, wie Daten angezeigt werden, wenn der Bericht generiert wird.
- **Bericht entfernen** Löschen Sie die Berichtsdefinition vom Berichtsserver.

Wenn Sie einen Berichtsordner auswählen, sind die folgenden Optionen verfügbar:

- **Neuer Ordner** Erstellen Sie einen neuen Ordner innerhalb des von Ihnen ausgewählten Ordners.
- **Ordnereigenschaften** Zeigen Sie die Eigenschaften des Ordners an oder ändern Sie diese.
- **Sicherheitseinstellungen** Kontrollieren Sie den Benutzerzugriff auf den Ordner, indem Sie Benutzern oder Gruppen die entsprechenden Rollen in SSRS zuweisen.
- **Berichte organisieren** Passen Sie die Struktur der Ordner an und ordnen Sie die Berichte nach Ordnern an.
- **Ordner löschen** Löschen Sie den Ordner sowie dessen gesamten Inhalt.

Um einen Bericht zu suchen, können Sie ihn nach dessen Namen suchen. Klicken Sie auf die Registerkarte „Suchen" im linken Bereich des Quest Knowledge Portal-Fensters, um eine Seite anzuzeigen, auf der Sie einen Namen eingeben können, und starten Sie dann Ihre Suche.

Weitere Informationen und Anweisungen finden Sie in der Hilfe von Quest Knowledge Portal. Um während der Verwendung von Quest Knowledge Portal Hilfethemen anzuzeigen, klicken Sie auf die Verknüpfung **Hilfe**.

Arbeiten mit Berichten

Der ActiveRoles Server Collector wird für die Vorbereitung von Daten zu Berichtszwecken verwendet. Die Daten werden in der von Ihnen bei der Konfiguration des Datenerfassungsauftrags angegebenen Datenbank gespeichert (siehe „Datenvorbereitungs-Collector für Berichte" weiter oben in diesem Kapitel). Um die Daten für den Berichtsserver verfügbar zu machen, muss die Datenquelle auf dem Berichtsserver so konfiguriert werden, dass sie eine Verbindung zu der Datenbank herstellt, in der sich die Berichtsdaten befinden. Dann können Sie ActiveRoles Server-Berichte generieren und anzeigen.

Konfigurieren der Datenquelle

Normalerweise wird die Datenquelle während der Installation von Report Pack konfiguriert. Wenn die Datenquelle nicht auf diese Weise konfiguriert wurde oder die Konfiguration der Datenquelle geändert werden muss, dann befolgen Sie die nachfolgend aufgeführten Anweisungen. Die Anweisungen setzen voraus, dass ActiveRoles Server Report Pack auf dem Berichtsserver installiert ist, den Sie konfigurieren möchten.

Gehen Sie folgendermaßen vor, um die Datenquelle mit Hilfe von SSRS Report Manager zu konfigurieren:

1. Starten Sie SSRS Report Manager und rufen Sie die Seite **Inhalt** auf.

   Report Manager wird während der Einrichtung von SQL Server Reporting Services (SSRS) auf demselben Computer wie der Berichtsserver installiert. Um Report Manager zu starten, öffnen Sie Microsoft Internet Explorer 6.0 oder höher. Geben Sie in das Adressfeld von Internet Explorer den Report Manager URL ein. Standardmäßig lautet der URL http://<Computername>/reports.

2. Gehen Sie auf der Seite **Inhalt** folgendermaßen vor:
   a) Klicken Sie auf **QKP**.
   b) Klicken Sie auf **SharedDatasources**.
   c) Klicken Sie auf die Datenquelle mit dem Namen **ActiveRoles Server 6.5.0 Berichtsdaten**.

   *Wenn das Element **SharedDatasources** nicht auf der Seite **Inhalt** angezeigt wird, klicken Sie auf **Details anzeigen**.*

3. Geben Sie auf der Seite **Eigenschaften** im Feld **Verbindungszeichenkette** die SQL Server-Instanz und den Namen der Datenbank, in der sich die von ActiveRoles Server Collector vorbereiteten Berichtsdaten befinden, an.

   Wenn der Name der Datenbank zum Beispiel „ARServerReporting" lautet und sich die Datenbank auf der SQL Server-Instanz mit dem Namen „MyServer\Enterprise" befindet, dann lautet die Verbindungszeichenkette wie folgt:

   ```
   data source = MyServer\Enterprise; initial catalog = ARServerReporting
   ```

4. Klicken Sie auf **Anwenden**.

Wenn Quest Knowledge Portal installiert ist, können Sie die Datenquelle mit Hilfe von Quest Knowledge Portal konfigurieren.

Gehen Sie folgendermaßen vor, um die Datenquelle mit Hilfe von Quest Knowledge Portal zu konfigurieren:

1. Öffnen Sie die Knowledge Portal-Startseite.

   Um die Knowledge Portal-Startseite zu öffnen, geben Sie den Knowledge Portal-URL in das Adressfeld von Internet Explorer ein. Standardmäßig lautet der URL http://<Computername>/QKP.

2. Klicken Sie im linken Bereich des Knowledge Portal-Fensters auf **Datenquellen** und wählen Sie die Datenquelle mit dem Namen **ActiveRoles Server 6.5.0 Report Data** aus.
3. Klicken Sie im rechten Bereich auf **Datenquelle ändern**.
4. Folgen Sie den Anweisungen des Assistenten.
5. Gehen Sie auf der Seite **Authentifizierungsmodus auswählen** im Assistenten wie folgt vor:
   a) Geben Sie die SQL Server-Instanz an, auf der sich die Datenbank befindet, die die Berichtsdaten enthält.
   b) Wählen Sie die für die Verbindung zur Datenbank zu verwendende Authentifizierungsmethode aus. Geben Sie bei Bedarf Anmeldeinformationen für den Zugriff ein.
6. Wählen Sie auf der Seite **Datenbank auswählen** die Datenbank aus, die die Berichtsdaten enthält.
7. Stellen Sie auf der Seite **Produkte auswählen** sicher, dass das Kontrollkästchen **ActiveRoles Server** aktiviert ist.
8. Schließen Sie den Assistenten ab.

Generieren und Anzeigen eines Berichts

Sie können ActiveRoles Server-Berichte mit Hilfe von SSRS Report Manager oder dem Quest Knowledge Portal generieren und als Vorschau anzeigen. Dieser Abschnitt enthält grundlegende Anweisungen bezüglich der Verwendung von Report Manager oder des Knowledge Portals für diesen Zweck.

Die folgenden Anweisungen setzen voraus, dass Berichtsdaten mit Hilfe von ActiveRoles Server Collector vorbereitet wurden und dass die Datenquelle auf dem Berichtsserver so konfiguriert wurde, dass eine Verbindung mit der Datenbank besteht, in der die Berichtsdaten gespeichert sind.

Gehen Sie folgendermaßen vor, um einen Bericht mit Hilfe von SSRS Report Manager anzuzeigen:

1. Starten Sie SSRS Report Manager und rufen Sie die Seite **Inhalt** auf.
2. Klicken Sie auf der Seite **Inhalt** auf **QKP**.
3. Finden Sie einen Bericht, indem Sie die Ordner durchsuchen oder den Bericht anhand seines Namens suchen.

   *Durchsuchen Sie die Ordnerinhalte, indem Sie auf einen Ordnernamen oder auf ein Ordnersymbol auf der Seite **Inhalt** klicken. Suchen Sie nach einem Bericht, indem Sie den gesamten Berichtsnamen oder einen Teil des Namens in das Textfeld **Suchen nach** oben auf der Seite eingeben.*

4. Klicken Sie auf den Namen eines Berichts, um den Bericht anzuzeigen.

   Einige Berichte erfordern die Eingabe von Parameterwerten. Sie können auch Filter anwenden, um anzugeben, welche Daten der Bericht enthalten soll.

5. Klicken Sie auf die Schaltfläche „Bericht anzeigen" oben auf der Seite.

Detaillierte Anweisungen bezüglich der Verwendung von Report Manager finden Sie in Microsoft SQL Server Books Online.

Gehen Sie folgendermaßen vor, um einen Bericht mit Hilfe von Quest Knowledge Portal anzuzeigen:

1. Klicken Sie im linken Bereich des Knowledge Portal-Fensters auf **Berichte** und suchen Sie dann einen Bericht, indem Sie Ordner durchsuchen.
2. Wählen Sie den Bericht im linken Bereich aus und klicken Sie dann auf **Bericht anzeigen** im rechten Bereich.

Nach der Erstellung wird der Bericht im Berichtsvorschaubereich angezeigt. Der Vorschaubereich umfasst eine Berichts-Symbolleiste, die über dem Bericht angezeigt wird, sodass Sie durch die Berichtsseiten blättern, eine Suche innerhalb eines Berichts ausführen oder den Bericht in einem anderen Format exportieren können.

Detaillierte Anweisungen bezüglich der Installation, Konfiguration und Verwendung von Quest Knowledge Portal finden Sie in der im Lieferumfang dieses Produkts enthaltenen Dokumentation.

Inhalt von ActiveRoles Server Report Pack

Dieser Abschnitt enthält eine Liste der Berichte, die mit Hilfe von ActiveRoles Server Pack vorbereitet werden können. Die Liste ist in Unterabschnitte gegliedert. Die Überschrift jedes Unterabschnitts gibt den Pfad zu einem bestimmten Berichtsordner an, wobei sich die Berichte in dem Ordner befinden, der unter der Überschrift des Unterabschnitts aufgeführt ist.

Active Directory-Bewertung/Domänen/

- Domänen – Zusammenfassung
- Domänen-Vertrauensstellungen
- Domänenkonto-SID-Auflösung

Active Directory-Bewertung/Benutzer/Kontoinformationen/

- Benutzerkontoliste
- Benutzerkontooptionen
- Kennwortalterinformationen
- Informationen über falsche Kennwörter

Active Directory-Bewertung/Benutzer/Exchange 2000/2003/

- Postfachinformationen nach Benutzern
- E-Mail-Übermittlungseinschränkungen
- E-Mail-Übermittlungsoptionen

Active Directory-Bewertung/Benutzer/Alte Konten/

- Deaktivierte Benutzerkonten
- Abgelaufene Benutzerkonten
- Inaktive Benutzerkonten
- Gesperrte Benutzerkonten
- Benutzerkonten mit abgelaufenem Kennwort
- Alle eingestellten Benutzerkonten
- Deprovisionierte Benutzerkonten

Active Directory-Bewertung/Benutzer/Verschiedene Informationen/

- Benutzer mit angegebenen Eigenschaften
- Benutzerprofilinformationen
- Vom Benutzer verwaltete Objekte
- Persönliche Hierarchie

Active Directory-Bewertung/Gruppen/

- Domänengruppenstatistik
- Gruppenliste mit Mitgliederstatistiken
- Gruppenhierarchie
- Leere Gruppen

Active Directory-Bewertung/Gruppenmitgliedschaft/

- Gruppenmitgliedschaft nach Gruppen
- Gruppenmitgliedschaft nach Benutzern
- Benutzer mit administrativen Rechten für Domänen

Active Directory-Bewertung/Organisationseinheiten/

- Mitgliederstatistik nach Organisationseinheiten
- Mitgliedschaft in Organisationseinheiten
- Hierarchie der Organisationseinheit

Active Directory-Bewertung/Andere Verzeichnisobjekte/

- Active Directory-Objekteigenschaften
- Computerkonten
- Alle eingestellten Computerkonten

ActiveRoles Server-Verlaufsprotokoll/Active Directory-Verwaltung

- Benutzerattributverwaltung
- Verzeichnisobjektverwaltung
- Deprovisionierung von Benutzerkonten

ActiveRoles Server-Verlaufsprotokoll/ActiveRoles Server-Ereignisse/

- ActiveRoles Server-Startfehler
- ActiveRoles Server-Ereignisstatistik

ActiveRoles Server-Verlaufsprotokoll/ActiveRoles Server-Konfigurationsänderungen/

- Delegation der Kontrolle
- Richtlinienerzwingung

ActiveRoles Server-Verlaufsprotokoll/ActiveRoles Server-Arbeitsablauf/

- Genehmigungen und Ablehnungen
- Arbeitsablauf-Überwachung

Administratorfunktionen/

- Mit verwalteten Einheiten verbundene Zugriffsvorlagen
- Mit Organisationseinheiten verbundene Zugriffsvorlagen
- Zugriffsvorlagenberechtigungen
- Zugriffsvorlagen – Zusammenfassung
- Delegation der Kontrolle nach Objekten (mit Gruppenhierarchie)
- Delegation der Kontrolle nach Objekten
- Delegation der Kontrolle nach Trustees
- Delegation der Kontrolle nach Trustees (mit Containerhierarchie)

Verwaltete Einheiten/

- Von der Richtlinie betroffene verwaltete Einheiten
- Mitglieder der verwalteten Einheit
- Mitgliedschaftsregeln für die verwaltete Einheit
- Verwaltete Einheit – Zusammenfassung
- Verwaltete Einheiten mit delegierter Kontrolle

Richtlinienobjekte/

- Richtlinienobjekte mit sicherbaren Objekten
- Richtlinienobjektreferenzen
- Richtlinienobjekteinstellungen
- Richtlinienobjekt – Zusammenfassung
- Einstellungen für die Auswertung der verknüpften Eigenschaft
- Einstellungen für die Auswertung der verknüpften Eigenschaft (mit Vererbung)
- Sicherbare Objekte (mit Vererbung)

Richtlinienkonformität/

- Verletzte Richtlinienregeln
- Objekte, die gegen die Richtlinienregeln verstoßen

12

Verwaltungsverlauf

- Beschreibung des Verwaltungsverlaufs
- Konfiguration des Verwaltungsverlaufs
- Untersuchen des Änderungsverlaufs
- Untersuchen von Benutzeraktivitäten

Beschreibung des Verwaltungsverlaufs

Die Funktion für den Verwaltungsverlauf stellt Informationen dazu bereit, welcher Benutzer zu welchem Zeitpunkt welche Verwaltungsaufgaben für Active Directory mit Hilfe von ActiveRoles Server ausgeführt hat.

Diese Funktion stellt ein gut verständliches Protokoll bereit, das die an einem bestimmten Objekt vorgenommenen Änderungen dokumentiert, wie etwa an einem Benutzer- oder Gruppenobjekt. Das Protokoll enthält detaillierte Einträge zu den ausgeführten Aktionen, zum Erfolg oder Fehler jeder Aktion sowie zu den geänderten Attributen.

Mit Hilfe des Verwaltungsverlaufs können Sie Folgendes untersuchen:

- **Verlauf ändern** Informationen zu Änderungen an Verzeichnisdaten, die über ActiveRoles Server vorgenommen wurden.
- **Benutzeraktivität** Informationen zu Verwaltungsaktionen, die ein bestimmter Benutzer ausgeführt hat.

Sowohl „Änderungsverlauf" als auch „Benutzeraktivität" verwenden dieselbe Informationsquelle – das Verwaltungsverlaufsprotokoll, das auch als Änderungsverfolgungsprotokoll bezeichnet wird. Die Konfigurationseinstellungen des Änderungsverfolgungsprotokolls werden weiter unten in diesem Kapitel beschrieben (siehe „Konfiguration des Verwaltungsverlaufs").

ActiveRoles Server umfasst auch Berichte, um den Verwaltungsverlauf durch die Erfassung und Analyse von Ereignisprotokolleinträgen zu untersuchen (siehe „Berichterstattung von ActiveRoles Server" weiter oben in diesem Dokument). Das Abrufen und Konsolidieren von Datensätzen aus dem Ereignisprotokoll kann zeitaufwändig und ineffizient sein.

Überlegungen und optimale Vorgehensweisen

In diesem Abschnitt werden Informationen und Empfehlungen bereitgestellt, die Sie berücksichtigen sollten, wenn Sie beabsichtigen, die Funktion für den Verwaltungsverlauf zu verwenden.

Diese Funktion soll Ihnen ermöglichen, umgehend zu untersuchen, welche Änderungen vor kurzem an den Verzeichnisdaten vorgenommen wurden, und zwar wann und von welchem Benutzer. Diese Funktion ist prinzipiell weder für die Überwachung von Datenänderungen bestimmt noch für die Untersuchung großer Mengen von Datenänderungen, die in einem langen Zeitraum aufgetreten sind.

Deshalb stellt ActiveRoles Server zusätzlich zu der Funktion für den Verwaltungsverlauf eine Folge von Berichten für die Nachverfolgung und Überwachung von Änderungen dar. Diese gehört zum Berichterstattungspaket von ActiveRoles Server. Außerdem ist das InTrust Knowledge Pack erhältlich, mit dem ActiveRoles Server sehr große Protokolle der Änderungsnachverfolgung verarbeiten und analysieren kann. Das Produkt InTrust wird separat von ActiveRoles Server verkauft.

Jede dieser drei Optionen (Verwaltungsverlauf, Berichterstattungspaket und Knowledge Pack) hat eigene Vorteile und Grenzen. Befolgen Sie die Empfehlungen in diesem Abschnitt, um die Option auszuwählen, die Ihren Anforderungen am besten entspricht.

Mit der Funktion für den Verwaltungsverlauf können Sie Änderungen untersuchen, die mit ActiveRoles Server an den Verzeichnisdaten vorgenommen wurden. Diese Funktion soll Ihnen helfen, die folgenden häufigen Fragen zu beantworten:

- Wer hat die letzten Änderungen an einem bestimmten Benutzer- oder Gruppenobjekt vorgenommen?
- Wer hat ein bestimmtes Benutzer- oder Gruppenobjekt in den letzten X Tagen geändert?
- Welche Änderungen wurde gestern Abend (gestern, vorgestern) an einem bestimmten Benutzerobjekt vorgenommen?
- Wurden geplante Änderungen an einem bestimmten Benutzer- oder Gruppenobjekt wirklich ausgeführt?
- Welche Objekte hat ein bestimmter delegierter Administrator in den letzten X Tagen geändert?

Sie können sofort auf den Verwaltungsverlauf zugreifen, wenn Sie ein Problem schnell untersuchen oder behandeln möchten, das aus ungeeigneten Änderungen von Verzeichnisdaten resultiert.

Die Funktion für den Verwaltungsverlauf schließt ein ausschließlich für sie verwendetes Repository ein, in dem Informationen zu Datenänderungen gespeichert werden. Dieses Repository wird als Verfolgungsprotokoll bezeichnet. Außerdem schließt sie eine spezielle grafische Benutzeroberfläche ein, über die Sie Informationen aus dem Repository abrufen und anzeigen können. Es sind keine zusätzlichen Aktionen erforderlich, wie etwa das Sammeln oder Konsolidieren von Informationen, um Verwaltungsverlaufs-Ergebnisse anhand des Verfolgungsprotokolls zu erstellen.

Die Vorteile der Funktion für den Verwaltungsverlauf bringen jedoch auch einige Einschränkungen mit sich. Bevor Sie die Funktion für den Verwaltungsverlauf verwenden, sollten Sie die folgenden empfohlenen optimalen Vorgehensweisen sowie Grenzen dieser Funktion überdenken.

Das Verfolgungsprotokoll ist in gewisser Weise unvollständig, da es keine Datenänderungen widerspiegelt, die von bestimmten Richtlinien gemacht werden, z.B. von der Richtlinie „Automatische Bereitstellung der Gruppenmitgliedschaft". Wenn eine solche Richtlinie Benutzer zu Gruppen hinzufügt oder daraus entfernt, fehlen Informationen zu diesen Richtlinienaktionen im Protokoll und somit auch in den Verwaltungsverlaufs-Ergebnissen. Wenn Sie Informationen zu allen Datenänderungen benötigen, auch zu denen, die durch Richtlinienaktionen ausgelöst wurden, sollten Sie Nachverfolgungsberichte für Änderungen verwenden. Diese werden weiter unten in diesem Abschnitt diskutiert.

Ein weiterer Faktor, den Sie beachten sollten, ist die Größe des Verfolgungsprotokolls. Um sicherzustellen, dass das Protokoll für alle Verwaltungsdienste in Echtzeit aktualisiert wird, wird es normalerweise in der Konfigurationsdatenbank von ActiveRoles Server gespeichert. Diese führt zu einer Begrenzung der Protokollgröße.

Standardmäßig ist das Verfolgungsprotokoll so konfiguriert, dass nur Informationen zu Änderungen in den letzten 30 Tagen gespeichert sind. Wenn Sie diese Einstellung erhöhen, lassen Sie Vorsicht walten; andernfalls können die folgenden Probleme auftreten:

- Eine übermäßige Erhöhung der Protokollgröße erhöht den Zeitaufwand für das Erstellen und Anzeigen von Änderungsverlauf- und Benutzeraktivitätsergebnissen erheblich.
- Wenn das Protokoll vergrößert wird, steigt die Größe der Konfigurationsdatenbank mit. Dies erhöht die zum Sichern und Wiederherstellen der Datenbank erforderliche Zeit beträchtlich und verursacht hohen Netzwerk-Datenverkehr bei der Replikation der Datenbank, wenn Sie der ActiveRoles Server-Replikation einen weiteren Verwaltungsdienst hinzufügen.
- Auf der grafischen Benutzeroberfläche können umfangreiche Verwaltungsverlaufs-Ergebnisse nicht überschaubar dargestellt werden. Da keine Filter- oder Seitenumbruchsfunktionen vorhanden sind, kann es unpraktisch und schwierig sein, die Ergebnisse strukturiert durchzusehen.

Um diese Einschränkungen zu überwinden, stellt Ihnen ActiveRoles Server ein anderes Hilfsmittel für die Überwachung von Änderungen bereit, die Nachverfolgungsberichte für Änderungen. Diese sind Teil des Berichterstattungspaket von ActiveRoles Server. Diese Berichte sollen Ihnen helfen, die folgenden Fragen zu beantworten:

- Welche Verwaltungsaufgaben wurden in einem bestimmten Zeitraum für ein bestimmtes Objekt ausgeführt?
- Welche Verwaltungsaufgaben wurden für ein bestimmtes Objekt während seiner gesamten Lebensdauer ausgeführt?
- Wann wurde ein bestimmtes Attribut eines bestimmten Objekts geändert?

Für die Arbeit mit Berichten bietet ActiveRoles Server eine erweiterte Berichterstattungslösung. Sie können Berichte mit umfangreichen Daten leicht verwalten: Konfigurieren Sie Filter und wenden Sie diese an, durchsuchen Sie die einzelnen Seiten und exportieren Sie Berichte in einer Vielzahl von Formaten.

Diese Berichte basieren auf Daten, die aus Ereignisprotokollen gesammelt werden. Auf jedem Computer mit dem Verwaltungsdienst wird ein separates Protokoll gespeichert. Jedes dieser Protokolle enthält nur Ereignisse, die der jeweilige Verwaltungsdienst generiert hat. Daher müssen Sie zum Verwenden von Berichten zunächst Ereignisse aus allen Ereignisprotokollen konsolidieren, sodass sie ein vollständiges Prüfprotokoll bilden.

Die Konsolidierung der Ereignisse, die als Datensammlungsprozess bezeichnet wird, wird von einer separaten Komponente von ActiveRoles Server ausgeführt, dem Collector. Mit dem Assistenten „Collector" können Sie Datensammlungsaufträge konfigurieren und ausführen sowie regelmäßige Ausführungen für sie planen.

Die wesentliche Einschränkung bei Nachverfolgungsberichten für Änderungen wird dadurch bedingt, dass Informationen in einer separaten Datenbank gesammelt und konsolidiert werden müssen, bevor Sie die Berichte vorbereiten können. Der Datensammlungsprozess weist folgende Nachteile auf:

- Der Datensammlungsvorgang kann sehr lange dauern, und die Datenbank kann inakzeptabel vergrößert werden, wenn Sie alle Ereignisse sammeln, die während eines langen Zeitraums in einer großen Umgebung aufgetreten sind.
- Daten können nicht über langsame WAN-Links gesammelt werden. Diese Einschränkung ist durch die Komponente von ActiveRoles Server bedingt, die Daten für die Berichterstattung sammelt.

Wenn Sie an diese Grenzen stoßen, können Sie das InTrust Knowledge Pack für ActiveRoles Server verwenden, um Ereignisprotokolle von Computern, auf denen der Verwaltungsdienst ausgeführt wird, zu konsolidieren und zu analysieren. Mit dem Knowledge Pack können sehr umfangreiche Nachverfolgungsdaten gespeichert, verwaltet und analysiert werden. Dieses Produkt verwendet komplexe Techniken, um Informationen aus Ereignisprotokollen zu sammeln und zu konsolidieren, sogar über langsame WAN-Verbindungen.

Konfiguration des Verwaltungsverlaufs

Die Konfiguration des Verwaltungsverlaufs umfasst die folgenden Elemente:

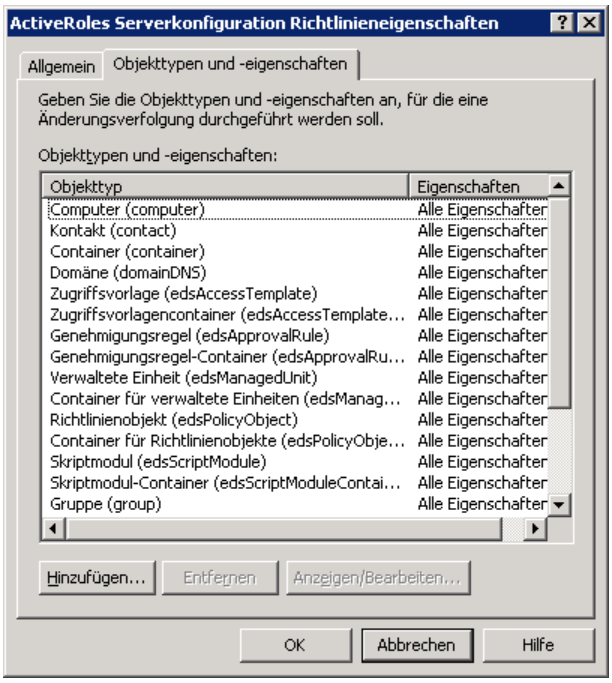
- **Richtlinie für die Änderungsnachverfolgung** Stellt zum Verlauf der Änderungen an Verzeichnisobjekten gehörende Daten zusammen legt fest, welche Änderungen in Berichte über den Änderungsverlauf und über Benutzeraktivitäten aufgenommen werden.
- **Konfiguration des Änderungsverfolgungsprotokolls** Gibt an, wie viele Änderungsanforderungen im Protokoll gespeichert werden sollen.
- **Replikation von Verwaltungsverlaufsdaten** Gibt an, ob Verwaltungsverlaufsdaten zwischen Verwaltungsdiensten, die verschiedene Datenbanken verwenden, synchronisiert werden soll oder nicht.

In den folgenden Abschnitten werden alle diesen Elemente ausführlich beschrieben.

Richtlinie für die Änderungsnachverfolgung

Das Verhalten der Verwaltungsverlaufsfunktion wird von der Richtlinie definiert, die im integrierten Richtlinienobjekt **Built-in Policy – Change Tracking** definiert ist. Die Richtlinie bestimmt die Objekttypen und -eigenschaften, für die Informationen zum Verwaltungsverlauf gesammelt werden sollen.

Um die Richtlinie anzuzeigen oder zu ändern, rufen Sie das Dialogfeld **Eigenschaften** für das Richtlinienobjekt **Built-in Policy – Change Tracking** (im Container **Configuration/Policies/Administration/Builtin**) und dann die Registerkarte **Richtlinien** auf, wählen Sie die Richtlinie aus und klicken Sie dann auf **Anzeigen/Bearbeiten**. Nun wird das Dialogfeld **Richtlinieneigenschaften** angezeigt. Die Registerkarte **Objekttypen und -eigenschaften** in diesem Dialogfeld sollte der folgenden Abbildung entsprechen.



Auf der Registerkarte werden die Objekttypen und -eigenschaften aufgelistet, die in den Verwaltungsverlauf eingeschlossen werden. Jeder Eintrag in der Liste schließt die folgenden Informationen ein:

- **Objekttyp** Wenn ein Objekt dieses Typs über ActiveRoles Server geändert wird, werden Informationen zu dieser Aktion im Änderungsverfolgungsprotokoll aufgezeichnet, sofern die Änderung sich auf eine in der Spalte **Eigenschaften** angegebene Eigenschaft auswirkt.
- **Eigenschaften** Informationen über Änderungen an diesen Eigenschaften werden im Änderungsverfolgungsprotokoll aufgezeichnet.

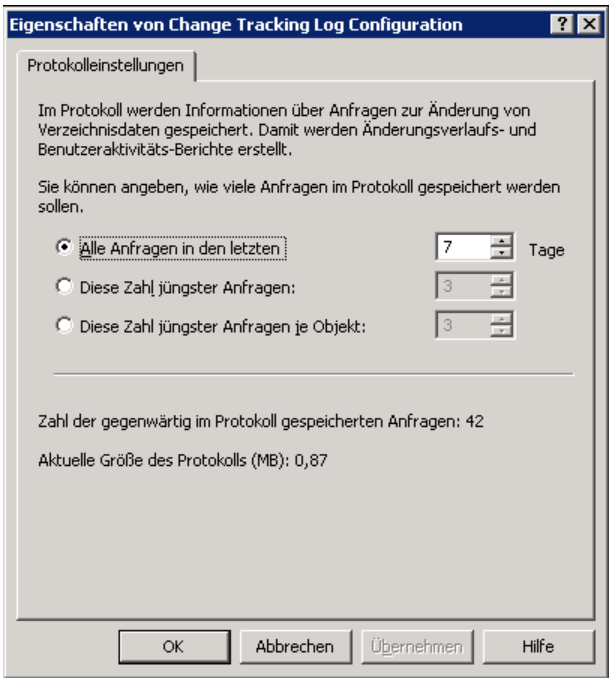
Sie können die Liste auf der Registerkarte mit Hilfe der Schaltflächen unter der Liste wie folgt verwalten:

- **Hinzufügen** Zeigt das Dialogfeld an, in dem Sie den Objekttyp und die Eigenschaften anzeigen können, die Sie in den Verwaltungsverlauf einschließen möchten. Sie können entweder einzelne oder alle Eigenschaften auswählen.
- **Entfernen** Löscht die ausgewählten Einträge aus der Liste.
- **Anzeigen/Bearbeiten** Zeigt das Dialogfeld an, in dem Sie die Eigenschaften für den ausgewählten Listeneintrag anzeigen und ändern können.

Konfiguration des Änderungsverfolgungsprotokolls

Eine weitere Konfigurationseinstellung für den Verwaltungsverlauf bestimmt die Größe des Verfolgungsprotokolls. In dem Protokoll werden Informationen zu Anforderungen zur Änderung von Verzeichnisdaten gespeichert, ein Datensatz pro Anforderung. Jeder Datensatz enthält Informationen zu den Änderungen an einem bestimmten Objekt, die gemäß einer bestimmten Änderungsanforderung vorgenommen wurden.

Sie können die Maximalanzahl von Datensätzen konfigurieren, indem Sie Verwaltungsfunktionen für Eigenschaften des Objekts **Konfiguration des Verfolgungsprotokolls ändern** verwenden. Dieses befindet sich im Container **Configuration/Server Configuration**. Die Registerkarte **Protokolleinstellungen** im Dialogfeld **Eigenschaften** für dieses Objekt sollte der folgenden Abbildung entsprechen.


Eigenschaften von Change Tracking Log Configuration
Protokolleinstellungen
Im Protokoll werden Informationen über Anfragen zur Änderung von Verzeichnisdaten gespeichert. Damit werden Änderungsverlaufs- und Benutzeraktivitäts-Berichte erstellt.
Sie können angeben, wie viele Anfragen im Protokoll gespeichert werden sollen.
Alle Anfragen in den letzten
7
Tage
Diese Zahl jüngster Anfragen:
3
Diese Zahl jüngster Anfragen je Objekt:
3
Zahl der gegenwärtig im Protokoll gespeicherten Anfragen: 42
Aktuelle Größe des Protokolls (MB): 0,87
OK
Abbrechen
Übernehmen
Hilfe

Auf der Registerkarte **Protokolleinstellungen** können Sie eine der folgenden Optionen auswählen:

- **Alle Anfragen in den letzten** *Anzahl* **Tage** Informationen über Änderungsanforderungen werden in das Protokoll geschrieben, sodass neue Anforderung die Anforderungen ersetzen, die älter als die angegebene Anzahl von Tagen sind.
- **Diese Zahl jüngster Anfragen** Für jedes Objekt werden im Protokoll höchstens so viele Änderungsanforderungen gespeichert wie angegeben. Wenn der Grenzwert erreicht ist, ersetzt jede neue Anforderung zur Änderung von Verzeichnisdaten die älteste Anforderung im Protokoll.
- **Diese Zahl jüngster Anfragen je Objekt** Für jedes Objekt werden im Protokoll höchstens so viele Änderungsanforderungen gespeichert wie angegeben. Wenn der Grenzwert für ein bestimmtes Objekt erreicht ist, ersetzt jede neue Anforderung zur Änderung des Objekts die älteste, mit diesem Objekt in Verbindung stehende Anforderung. Die Gesamtzahl der Anforderungen hängt von der Anzahl der Objekte ab, die über ActiveRoles Server geändert werden.

Standardmäßig ist das Verfolgungsprotokoll so konfiguriert, dass Informationen zu Anforderungen in den letzten 30 Tagen gespeichert sind. Die Informationen über die Änderungsanforderungen werden in das Protokoll geschrieben, sodass neue Anforderungen solche Anforderungen ersetzen, die älter als 30 Tage sind. Wenn Sie diese Zahl erhöhen, lassen Sie Vorsicht walten. Wenn Sie diese Zahl deutlich erhöhen, wird auch das Protokoll umfangreicher. Wenn Sie beabsichtigen, diese Einstellung zu ändern, sollten Sie zunächst den Abschnitt „Überlegungen und optimale Vorgehensweisen" weiter oben in diesem Kapitel lesen.

Das Verfolgungsprotokoll wird als Informationsquelle für den Änderungsverlauf und den Verlauf zur Benutzeraktivität verwendet. Der Umfang der im Protokoll gespeicherten Anforderungen bestimmt den Wartezeitraum für den Änderungsverlauf sowie für die Benutzeraktivität.

Replikation von Verwaltungsverlaufsdaten

Standardmäßig werden die Verwaltungsverlaufsdaten in den ActiveRoles Server-Konfigurationsdatenbanken gespeichert. Wenn die ActiveRoles Server-Replikation also wie im Abschnitt „Konfigurieren von Replikationen" weiter unten in diesem Dokument beschrieben konfiguriert ist, werden die Verwaltungsverlaufdaten gemeinsam mit den anderen Konfigurationsdaten zwischen Verwaltungsdiensten repliziert. Bei einem hohen Verwaltungsverlaufs-Datenvolumen kann dies zu einer beträchtlichen Belastung des Netzwerks führen.

ActiveRoles Server gibt Ihnen die Möglichkeit, die Replikation von Verwaltungsverlaufsdaten zu deaktivieren, um die Belastung des Netzwerks zu verringern. Beachten Sie jedoch, dass dies dazu führt, dass jeder Datenbankserver einen eigenen Verwaltungsverlaufsdatenspeicher führt. Dies hat zur Folge, dass Sie den Verwaltungsverlauf verwenden können, um die Änderungen zu untersuchen, die nur über die Verwaltungsdienste vorgenommen wurden, die dieselbe Datenbank wie der Verwaltungsdienst, mit dem Sie verbunden sind, nutzen.

Die Deaktivierung der Replikation von Verwaltungsverlaufsdaten hat folgende Konsequenzen:

- Die durch den Befehl **Verlauf ändern** oder **Benutzeraktivität** generierten Informationen enthalten nur Informationen über die Änderungen, die mit Hilfe einer bestimmten Gruppe von Verwaltungsdiensten durchgeführt wurden (die Dienste, die eine gemeinsame Datenbank nutzen).

  Die die ActiveRoles Server-Konsole oder das Web-Interface automatisch den Dienst auswählen, zu dem eine Verbindung hergestellt wird, erhalten Sie während verschiedenen Verbindungssitzungen möglicherweise verschiedene Berichte für dasselbe Zielobjekt oder Benutzerkonto.

- Die Funktionen von ActiveRoles Server wie etwa der Genehmigungs-Arbeitsablauf, die Bestätigungsprüfung, temporäre Gruppenmitgliedschaften und das Rückgängig möchten der Deprovisionierung funktionieren möglicherweise nicht wie erwartet. Einige Vorgänge, die auf diesen Funktionen beruhen, können von Client-Schnittstellen, die mit anderen Verwaltungsdienste verbunden sind, nicht richtig verarbeitet oder angezeigt werden.

  ActiveRoles Server verwendet den Verwaltungsverlaufsspeicher zur Speicherung von Genehmigungs-, Bestätigungs- und Deprovisionsaufgaben sowie Aufgaben im Zusammenhang mit temporären Gruppenmitgliedschaften. Ohne Synchronisation der Informationen zwischen Verwaltungsverlaufsspeichern ist eine solche, von einem der Verwaltungsdienste erstellte Aufgabe möglicherweise nicht für andere Verwaltungsdienste verfügbar. Als Folge variiert das Verhalten der ActiveRoles Server-Konsole oder des Web-Interface abhängig vom gewählten Verwaltungsdienst.

Die Deaktivierung der Replikation des Verwaltungsverlaufsdaten hat keinen Einfluss auf die Replikation der anderen, mit der Konfiguration von ActiveRoles Server verbundenen Daten. Nur der Verwaltungsverlauf-relevante Teil der Konfigurationsdatenbank wird von der ActiveRoles Server-Replikation ausgeschlossen.

Die Anweisungen bezüglich der Deaktivierung der Replikation von Verwaltungsverlaufsdaten hängen davon ab, ob die ActiveRoles Server-Replikation bereits konfiguriert ist oder nicht.

Replikation noch nicht konfiguriert

Wenn Sie die ActiveRoles Server-Replikation erstmalig konfigurieren, können Sie sicherstellen, dass die Verwaltungsverlaufsdaten nicht bei der ActiveRoles Server-Replikation berücksichtigt werden, indem Sie die Rolle des „Herausgebers" wie folgt festlegen (eine Definition der Replikationsrollen finden Sie unter „Konfigurieren von Replikationen" weiter unten in diesem Dokument):

1. Stellen Sie über die ActiveRoles Server-Konsole eine Verbindung zu dem Verwaltungsdienst her, dessen SQL Server die Rolle als Herausgeber übernehmen soll.
2. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration | Server Configuration** und wählen Sie den Container **Configuration Databases**.
3. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf die Datenbank und klicken Sie dann auf **Heraufstufen**.
4. Warten Sie, bis die Konsole den Vorgang „Heraufstufen" ausführt.
5. Wählen Sie in der Konsolenstruktur unter **Server Configuration** den Container **Management History Databases**.
6. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf die Datenbank und klicken Sie dann auf **Herabstufen**.
7. Warten Sie, bis die Konsole den Vorgang „Herabstufen" abgeschlossen hat.

Dann können Sie die ActiveRoles Server-Replikation mittels der ActiveRoles Server-Konsole wie im Abschnitt „Konfigurieren von Replikationen" weiter unten in diesem Dokument beschrieben konfigurieren: Verwenden Sie den Befehl **Replikationspartner hinzufügen** für die Datenbank im Container **Konfigurationsdatenbanken**, um Abonnenten zu dem von Ihnen konfigurierten Herausgeber hinzuzufügen.

Replikation bereits konfiguriert

Dieser Abschnitt enthält Anweisungen bezüglich der Deaktivierung der Replikation von Verwaltungsverlaufsdaten für den Fall, dass die ActiveRoles Server-Replikation bereits wie im Abschnitt „Konfigurieren von Replikationen" weiter unten in diesem Dokument beschrieben konfiguriert ist. Sie müssen zunächst alle Abonnenten der Verwaltungsverlaufsdaten löschen und dann den Herausgeber für die Verwaltungsverlaufsdaten herabstufen. Hierdurch wird nur die Replikation der Verwaltungsverlaufsdaten gestoppt; die anderen Replikationsfunktionen bleiben erhalten.

Deaktivieren der Replikation von Verwaltungsverlaufsdaten:

1. Stellen Sie über die ActiveRoles Server-Konsole eine Verbindung zu dem Verwaltungsdienst her, dessen SQL Server die Rolle des Herausgebers inne hat.
2. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration | Server Configuration** und wählen Sie den Container **Management History Databases** aus.
3. Verwenden Sie den Befehl **Löschen** für jede der Abonnenten-Datenbanken, um alle Abonnenten im Container **Management History Databases** zu löschen.
4. Klicken Sie mit der rechten Maustaste auf die Herausgeber-Datenbank und klicken Sie dann auf **Herabstufen**.
5. Warten Sie, bis die Konsole den Vorgang „Herabstufen" abgeschlossen hat.

Neukonfiguration der Replikation von Verwaltungsverlaufsdaten

Wenn die Replikation von Verwaltungsverlaufsdaten deaktiviert ist, ist es immer noch möglich, dass mehrere Verwaltungsdienste dasselbe Änderungsverlaufsprotokoll verwenden, indem Sie sie so konfigurieren, dass sie dieselbe Datenbank nutzen. Beachten Sie, dass die Verwaltungsdienst-Version 6.x Ihnen ermöglicht, mehrere Dienste mit der Option, eine einzige Konfigurationsdatenbank zu nutzen, zu installieren. So können Sie den ersten Dienst in Ihrer Umgebung installieren und das Setup-Programm eine Datenbank erstellen lassen. Dann können Sie einen weiteren Dienst installieren, wobei das Setup-Programm den neuen Dienst so konfiguriert, dass dieser dieselbe Datenbank wie der vorhandene Dienst nutzt.

Wenn jedoch verschiedene Verwaltungsdienste in Ihrer Umgebung unterschiedliche Datenbankserver nutzen, müssen Sie die Replikation der Verwaltungsverlaufsdaten möglicherweise neu konfigurieren, um die Verwaltungsverlaufsfunktion mit all ihren Vorteilen nutzen zu können. Verwalten Sie zu diesem Zweck die Objekte im Container **Management History Databases** wie folgt:

Gehen Sie folgendermaßen vor, um die Replikation von Verwaltungsverlaufsdaten neu zu konfigurieren:

1. Stellen Sie über die ActiveRoles Server-Konsole eine Verbindung zu dem Verwaltungsdienst her, dessen SQL Server die Rolle als Herausgeber für Konfigurationsdaten inne hat.
2. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration | Server Configuration** und wählen Sie den Container **Management History Databases** aus.
3. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf die Datenbank und klicken Sie dann auf **Heraufstufen**.
4. Warten Sie, bis die Konsole den Vorgang „Heraufstufen" ausführt.
5. Verwenden Sie den Befehl **Replikationspartner hinzufügen** für die Herausgeber-Datenbank im Container **Management History Databases**, um Abonnenten für die Verwaltungsverlaufsdaten hinzuzufügen.

Der Befehl **Replikationspartner hinzufügen** startet den Assistenten, der nahezu identisch mit dem im Abschnitt „Hinzufügen von Mitgliedern zu einer Replikationsgruppe" weiter unten in diesem Dokument beschriebenen Assistenten ist. Der einzige Unterschied besteht darin, dass die Liste der Verwaltungsdienste, deren Datenbankserver als Abonnenten für die Verwaltungsverlaufsdaten angegeben werden können, auf die Dienste beschränkt ist, die dieselben, auf dem von Ihnen ausgewählten Herausgeber gehosteten Konfigurationsdaten nutzen.

Zentralisierte Verwaltungsverlaufsspeicherung

Bei Auswahl der Standard-Replikationseinstellungen in ActiveRoles Server werden die Verwaltungsverlaufsdaten zusammen mit den Konfigurationsdaten zwischen Replikationspartnern synchronisiert. Bei einem großen Volumen an Verwaltungsverlaufsdaten kann dieses Verhalten zu einer hohen Belastung des Netzwerks führen, was bei bestimmten Szenarien wie etwa beim Hinzufügen eines neuen Partners zur ActiveRoles Server-Replikationsgruppe Leistungseinbußen von ActiveRoles Server zur Folge haben kann. Hier finden Sie Anweisungen bezüglich der Vermeidung der Replikation von Verwaltungsverlaufsdaten durch die Implementierung einer gemeinsamen Speicherung dieser Daten für alle Replikationspartner.

Die Synchronisation der Verwaltungsverlaufsdaten kann vom ActiveRoles Server-Replikationsvorgang entfernt werden, indem Sie eine gemeinsame Speicherung dieser Daten für alle Replikationspartner implementieren. Die gemeinsame Speicherung gewährleistet die Konsolidierung der Teile der Verwaltungsverlaufsdaten, die von verschiedenen Verwaltungsdiensten generiert wurden, während sie gleichzeitig die Notwendigkeit einer Synchronisation dieser Daten zwischen mehreren Speichern vermeidet.

ActiveRoles Server bietet die folgenden Optionen, um einen zentralisierten, gemeinsamen Speicher für die Verwaltungsverlaufsdaten zu implementieren:

- Konfigurieren Sie die Verwaltungsdienste so, dass die Konfigurationsdatenbank eines dieser Dienste von den anderen Diensten als Verwaltungsverlaufsspeicher verwendet wird. Auf diese Weise verwenden alle Verwaltungsdienste, die eine gemeinsame Konfiguration nutzen, denselben Verwaltungsverlaufsspeicher – nämlich die Konfigurationsdatenbank, die Sie für diese Rolle auswählen.
- Erstellen Sie eine separate Datenbank, in der die Verwaltungsverlaufsdaten gespeichert werden sollen, und konfigurieren Sie dann die Verwaltungsdienste so, dass sie diese Datenbank anstelle Ihrer Konfigurationsdatenbank als den Verwaltungsverlaufsspeicher nutzen. Auf diese Weise verwenden alle Verwaltungsdienste, die eine gemeinsame Konfiguration nutzen, denselben Verwaltungsverlaufsspeicher – nämlich die von Ihnen erstellte Verwaltungsverlaufsdatenbank.

In diesem Abschnitt wird jede dieser beiden Optionen eingehend beschrieben.

Option 1: Dedizierte Konfigurationsdatenbank für die Speicherung der Verwaltungsverlaufsdaten

Standardmäßig speichert der Verwaltungsdienst sowohl seine Konfigurationsdaten als auch seine Verwaltungsverlaufsdaten in derselben Konfigurationsdatenbank. Folglich müssen bei mehreren Konfigurationsdatenbanken die Verwaltungsverlaufsdaten gemeinsam mit den Konfigurationsdaten per Replikation synchronisiert werden, um die Verwaltungsverlaufsdaten zu konsolidieren.

ActiveRoles Server bietet die Möglichkeit, die Verwaltungsdienste, die eine gemeinsame Konfiguration nutzen, neu zu konfigurieren, sodass eine einzige Konfigurationsdatenbank für die Speicherung der Verwaltungsverlaufsdaten für alle Verwaltungsdienste genutzt wird. Diese Option verleiht Ihnen die Flexibilität, die Speicherung von Konfigurationsdaten zu verteilen und gleichzeitig die Speicherung von Verwaltungsverlaufsdaten zu zentralisieren. Gehen Sie wie nachfolgend beschrieben vor, um dieses Szenario zu implementieren.

1. Deaktivieren Sie die Replikation von Verwaltungsverlaufsdaten. Sie können dazu die ActiveRoles Server-Konsole wie folgt verwenden: Stellen Sie eine Verbindung zu dem Verwaltungsdienst her, dessen Datenbankserver die Rolle des Herausgebers in der Replikationsgruppe inne hat, rufen Sie dann den Container **Configuration/Server Configuration/Management History Databases/** auf, löschen Sie alle Abonnentenobjekte aus diesem Container und führen Sie dann den Befehl **Herabstufen** für das Herausgeberobjekt in diesem Container aus.
2. Entscheiden Sie, welche Konfigurationsdatenbank als der gemeinsame Speicher für die Verwaltungsverlaufsdaten genutzt werden soll. In diesem Abschnitt wird die Datenbank, die Sie auswählen, als die *Verwaltungsverlaufsdatenbank* bezeichnet.
3. Für jeden Verwaltungsdienst, der seine Konfigurationsdaten in einer anderen Datenbank als in der von Ihnen im vorigen Schritt ausgesuchten Datenbank speichert, führen Sie die im Unterabschnitt „Konfigurieren des Verwaltungsdienstes, sodass dieser die neue Verwaltungsverlaufsdatenbank verwendet" weiter unten in diesem Abschnitt aufgeführten Schritte durch.

Option 2: Separate Konfigurationsdatenbank für die Speicherung der Verwaltungsverlaufsdaten

ActiveRoles Server bietet auch die Möglichkeit, die Verwaltungsverlaufsdaten in einer separaten Verwaltungsverlaufsdatenbank zu speichern, anstatt dieselbe Datenbank für die Speicherung der Konfigurationsdaten und der Verwaltungsverlaufsdaten zu verwenden. Bei Auswahl dieser Option können mehrere Verwaltungsdienste so konfiguriert werden, dass sie eine gemeinsame Verwaltungsverlaufsdatenbank auf einem dedizierten SQL Server verwenden.

Wenn eine Gruppe von Verwaltungsdiensten dieselbe Verwaltungsverlaufsdatenbank nutzen soll, müssen Sie gewährleisten, dass die Verwaltungsdienste in der Gruppe über dieselbe Konfiguration verfügen. Dies kann auf eine der folgenden Weisen erfolgen:

- Verwenden Sie die ActiveRoles Server-Replikationsfunktion, um die Konfigurationsdatenbanken zu synchronisieren, die von den Verwaltungsdiensten verwendet werden.
- Achten Sie darauf, dass alle Verwaltungsdienste in der Gruppe dieselbe Konfigurationsdatenbank nutzen.

Mit derselben Konfiguration für alle Verwaltungsdienste einschließlich der Konfiguration des Web-Interface und der verwalteten Domänen vermeiden Sie jegliche Inkonsistenzen in den Verwaltungsverlaufsdaten, die von den Verwaltungsdiensten gemeinsam genutzt werden.

Gehen Sie wie nachfolgend beschrieben vor, um das auf dieser Option beruhende Szenario zu implementieren.

1. Deaktivieren Sie die Replikation von Verwaltungsverlaufsdaten. Sie können dazu die ActiveRoles Server-Konsole wie folgt verwenden: Stellen Sie eine Verbindung zu dem Verwaltungsdienst her, dessen Datenbankserver die Rolle des Herausgebers in der Replikationsgruppe inne hat, rufen Sie dann den Container **Configuration/Server Configuration/Management History Databases/** auf, löschen Sie alle Abonnentenobjekte aus diesem Container und führen Sie dann den Befehl **Herabstufen** für das Herausgeberobjekt in diesem Container aus.
2. Erstellen Sie die Verwaltungsverlaufsdatenbank. Anweisungen hierzu finden Sie unter „Erstellen einer Verwaltungsverlaufsdatenbank" weiter unten in diesem Abschnitt.
3. Füllen Sie die neue Verwaltungsverlaufsdatenbank optional mit den Verwaltungsverlaufsdaten, die bereits in Ihrer ActiveRoles Server-Umgebung vorhanden sind. Anweisungen hierzu finden Sie unter „Importieren von Daten in die neue Verwaltungsverlaufsdatenbank" weiter unten in diesem Abschnitt.
4. Führen Sie für jeden Verwaltungsdienst die Schritte durch, die im Unterabschnitt „Konfigurieren des Verwaltungsdienstes, sodass dieser die neue Verwaltungsverlaufsdatenbank verwendet" weiter unten in diesem Abschnitt aufgeführt sind.

Erstellen einer Verwaltungsverlaufsdatenbank

Um eine Verwaltungsverlaufsdatenbank zu erstellen, verwenden Sie die SQL-Skripts, die sich im Ordner **Verschiedenes\MH-Datenbank erstellen** auf der ActiveRoles Server-CD befinden. Führen Sie auf dem Computer, auf dem SQL Server installiert ist, die Datei CreateDB.bat aus und führen Sie dann die Datei Create_MHOnly.bat aus. Jede dieser Dateien weist die folgenden Parameter auf:

- Erster Parameter (erforderlich). Gibt die SQL Server-Instanz in der Form *Computername* für eine Standardinstanz oder *Computername**Instanzname* für eine benannte Instanz an, auf der Sie die Datenbank erstellen möchten.
- Zweiter Parameter (erforderlich). Name der Datenbank, die Sie erstellen möchten.

- Dritter Parameter (optional). SQL Server-Login, mit dem Sie sich bei SQL Server anmelden möchten (impliziert die SQL Server-Authentifizierung). Wenn der dritte Parameter nicht angegeben wird, verwendet das Skript die Windows-Authentifizierung mit den Anmelde-informationen des aktuell angemeldeten Benutzers.
- Vierter Parameter (optional). Passwort des SQL Server-Logins. Geben Sie diesen Parameter nicht an, wenn das Login über ein leeres Kennwort verfügt.

Beispiel: Die folgende Befehlssequenz Erstellen der Datenbank mit dem Namen „ChangeHistory" in der Instanz „MyServer\ARS" von SQL Server, wobei der Vorgang im Sicherheitskontext des aktuell angemeldeten Benutzers durchgeführt wird:

```
CreateDB.bat „MyServer\ARS" „[ChangeHistory]"
Create_MHOnly.bat „MyServer\ARS" „ChangeHistory"
```

Um die Datenbank zu erstellen, geben Sie den ersten Befehl in der Eingabeaufforderung ein und warten Sie, während das Skript den Vorgang ausführt. Wenn der Vorgang CreateDB abgeschlossen ist, geben Sie den zweiten Befehl ein.

Importieren von Daten in die neue Verwaltungsverlaufsdatenbank

Sie müssen möglicherweise die neu erstellte Verwaltungsverlaufsdatenbank mit ihren vorhandenen Verwaltungsverlaufsdaten füllen, sodass die Daten für die ActiveRoles Server-Benutzerschnittstellen verfügbar bleiben, nachdem Sie den Verwaltungsdienst für die Verwendung der neuen Verwaltungs-verlaufsspeichers konfiguriert haben. Verwenden Sie hierzu den Verwaltungsverlauf-Migrations-Assistent, der Teil der ActiveRoles Server-Verwaltungsdienstinstallation ist.

Der Assistent führt die in den Quelldatenbanken gefundenen Verwaltungsverlaufsdaten wie etwa die ActiveRoles Server-Konfigurationsdatenbank mit den in der Verwaltungsverlaufsdatenbank gespeicherten Daten zusammen. Beachten Sie, dass der Assistent nur neue Daten hinzufügt und jegliche bereits in der Verwaltungsverlaufsdatenbank enthaltene Daten erhalten bleiben. Sie können die alten Verwaltungsverlaufsdaten jederzeit importieren, nachdem Sie den Verwaltungsdienst auf den neuen Verwaltungsverlaufsspeicher umgeleitet haben, ohne einen Datenverlust fürchten zu müssen.

Der Assistent fragt Sie zunächst nach der Datenbank, aus der Daten importiert werden sollen. Sie können Daten aus der Konfigurationsdatenbank importieren, die vom Verwaltungsdienst verwendet wird. Als nächstes fragt Sie der Assistent nach der Datenbank, in die Sie die Daten importiert möchten. Geben Sie die von Ihnen erstellte Verwaltungsverlaufsdatenbank an. Dann fragt Sie der Assistent, ob Sie alle Datensätze oder nur einen bestimmten Datensatzbereich importieren möchten. Sie können sich entscheiden, nicht alle Datensätze zu importieren, da der Import großer Datenmengen mehrere Stunden in Anspruch nehmen kann. Abschließend überträgt der Assistent die Daten. Ausführliche Anweisungen über die Verwendung des Assistenten finden Sie im Abschnitt „Importieren von Verwaltungsverlaufs-daten" im *ActiveRoles Server – Erste Schritte*.

Konfigurieren des Verwaltungsdienstes, sodass dieser die neue Verwaltungsverlaufsdatenbank verwendet

Gehen Sie wie nachfolgend beschrieben vor, um den Verwaltungsdienst auf den neuen Verwaltungsverlaufsspeicher umzuleiten.

1. Führen Sie auf dem Computer, auf dem der Verwaltungsdienst ausgeführt wird, den Befehl „regedit" aus, um den Registrierungsschlüssel **HKLM\Software\Aelita\Enterprise Directory Manager\CHDatabaseConnectionString** zu finden, und untersuchen Sie die Werte **Datenquelle** und **Startkatalog** in diesem Schlüssel:
   - **Datenquelle** gibt den Namen der SQL Server-Instanz an, die die Datenbank hostet, in der der Verwaltungsdienst aktuell die Verwaltungsverlaufsdaten speichert. Notieren Sie den Wert für **Datenquelle**.
   - **Startkatalog** gibt den Namen der Datenbank an, in der der Verwaltungsdienst aktuell die Verwaltungsverlaufsdaten speichert. Notieren Sie den Wert für **Startkatalog**.
2. Stoppen Sie den Verwaltungsdienst. Geben Sie hierzu den folgenden Befehl an der Eingabeaufforderung des Computers ein, auf dem der Verwaltungsdienst ausgeführt wird: **net stop arssvc**
3. Konfigurieren Sie die neuen Verbindungseinstellungen. Wechseln Sie an der Eingabeaufforderung zu dem ActiveRoles Server-Installationsverzeichnis (standardmäßig ist dies C:\Programme\Quest Software\ActiveRoles Server\), geben Sie einen Befehl auf der Grundlage der folgenden Syntax ein und führen Sie dann den Befehl aus.

   Befehlssyntax:

   ```
   arssvc.exe /dbMHServerName <Instanz> /dbMHName <Name> /dbMHAuthenticationMode
   <0 | 1> /dbMHLogin <Login> /dbMHPassword <Kennwort>
   ```

   Ersetzen Sie in dieser Syntax die Platzhalter durch die tatsächlichen Parameterwerte:

   - Ersetzen Sie in /dbMHServerName <Instanz> den Wert <Instanz> durch die Zeichenkette, die die SQL Server-Instanz angibt, die die neue Verwaltungsverlaufsdatenbank hostet. Geben Sie diese Zeichenkette in der Form *Computername* für eine Standardinstanz oder *Computername**Instanzname* für eine benannte Instanz an.
   - Ersetzen Sie in /dbMHName <Name> den Wert <Name> durch den Namen der Verwaltungsverlaufsdatenbank.
   - Geben Sie in /dbMHAuthenticationMode <0 | 1> entweder 0 oder 1 anstelle von <0 | 1> ein, um den Authentifizierungsmodus der Verwaltungsdienstverbindung mit der Verwaltungsverlaufsdatenbank festzulegen:
   - /dbMHAuthenticationMode 0 führt dazu, dass der Verwaltungsdienst die SQL Server-Authentifizierung verwendet (diese Einstellung erfordert, dass Sie auch die Parameter /dbMHLogin und /dbMHPassword angeben; der Verwaltungsdienst verwendet das angegebene Login und Kennwort für den Verbindungsaufbau zur Datenbank)
   - /dbMHAuthenticationMode 1 führt dazu, dass der Verwaltungsdienst die Windows-Authentifizierung verwendet (bei Auswahl von dieser Einstellung haben die Parameter /dbMHLogin und /dbMHPassword keinen Einfluss; der Verwaltungsdienst verwendet sein Dienstkonto für den Verbindungsaufbau zur Datenbank)
   - Ersetzen Sie in /dbMHLogin <Login> den Wert <Login> durch den Namen des SQL Server-Login, der für die SQL Server-Authentifizierung verwendet werden soll (dieser Parameter hat nur dann Auswirkungen, wenn /dbMHAuthenticationMode auf 0 gesetzt ist).
   - Ersetzen Sie in /dbMHPassword <Kennwort> den Wert <Kennwort> durch das Kennwort des SQL Server-Login (dieser Parameter hat nur dann Auswirkungen, wenn /dbMHAuthenticationMode auf 0 gesetzt ist).

Beispiel: Der folgende Befehl konfiguriert den Verwaltungsdienst so, dass er Verwaltungsverlaufsdaten in der Datenbank „ChangeHistory" in der MyServer\ARS-Instanz von SQL Server speichert, wobei der verwendete Authentifizierungsmodus auf Windows-Authentifizierung gesetzt ist:

```
arssvc.exe /dbMHServerName "MyServer\ARS" /dbMHName "ChangeHistory"
/dbMHAuthenticationMode 1
```

4. Aktualisieren Sie die Konfigurationsdatenbank des Verwaltungsdienstes, um einen Verweis auf den alten Verwaltungsverlaufsspeicher zu löschen. Verwenden Sie die folgende Syntax, um ein SQL-Skript zu erstellen, und führen Sie das SQL-Skript auf dem SQL Server aus, der die Konfigurationsdatenbank hostet, wobei Sie die Konfigurationsdatenbank als das Ziel auswählen:

   ```
   delete from MHPartners where edsaSQLAlias = '<Datenquelle>' und
   edsaDatabaseName = '<Anfangskatalog>'
   ```

   Ersetzen Sie in dieser Syntax die Platzhalter durch die tatsächlichen Werte:

   - Ersetzen Sie <Datenquelle> durch den Wert **Datenquelle**, den Sie in Schritt 1 notiert haben.
   - Ersetzen Sie <InitialCatalog> durch den Wert **Startkatalog**, den Sie in Schritt 1 notiert haben.

   Beispiel: Angenommen, der Wert **Datenquelle** ist auf MyServer\ARS und der Wert **Startkatalog** ist auf ARServer60 gesetzt. Bei diesen Werten sieht das SQL-Skript folgendermaßen aus:

   ```
   delete from MHPartners where edsaSQLAlias = 'MyServer\ARS' und edsaDatabaseName
   = 'ARServer60'
   ```

5. Aktualisieren Sie die Verwaltungsverlaufsdatenbank, um einen Verweis auf den Verwaltungsdienst zu erstellen. Verwenden Sie die folgende Syntax, um ein SQL-Skript zu erstellen, und führen Sie das SQL-Skript auf dem SQL Server aus, der die Verwaltungsverlaufsdatenbank hostet, wobei Sie die Verwaltungsverlaufsdatenbank als das Ziel auswählen:

   ```
   exec ProvideMHServiceEntry '<ARSDienstname>', 0, 0
   ```

   Ersetzen Sie in dieser Syntax <ARSDienstname> durch den vollqualifizierten DNS-Namen des Computers, auf dem der Verwaltungsdienst ausgeführt wird.

   Beispiel: Wenn ARSService.mycompany.com der Name des Computers ist, auf dem der Verwaltungsdienst ausgeführt wird, sieht das SQL-Skript folgendermaßen aus:

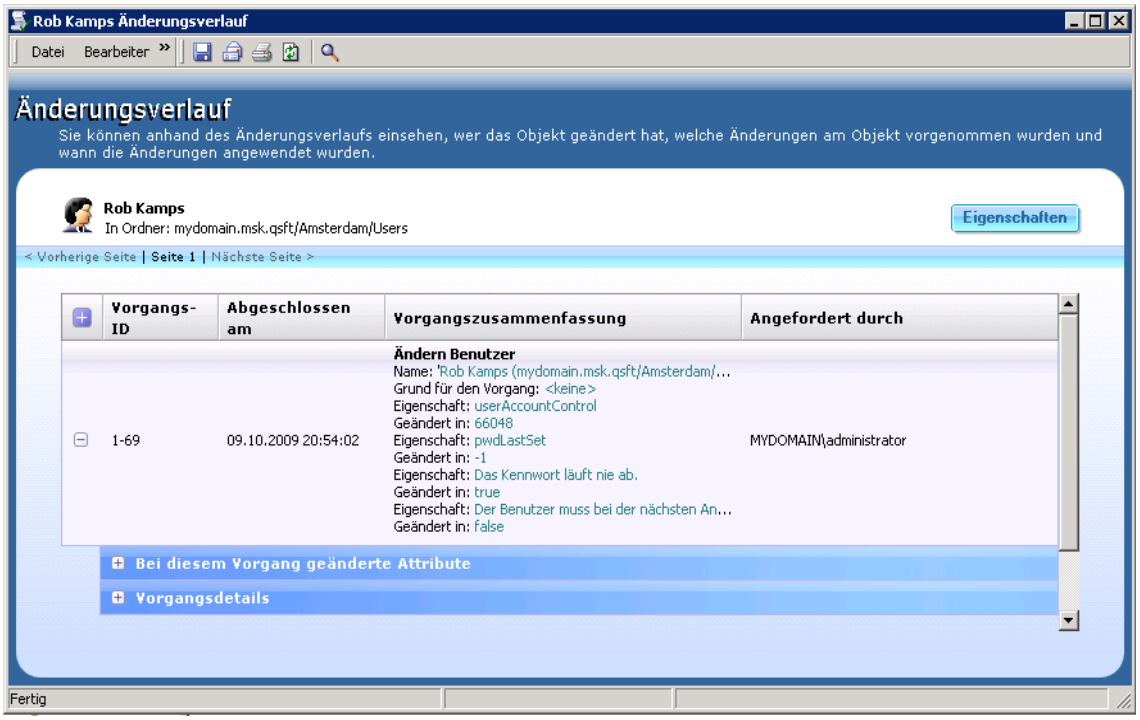
   ```
   exec ProvideMHServiceEntry 'ARSService.mycompany.com', 0, 0
   ```

6. Starten Sie den Verwaltungsdienst. Geben Sie hierzu den folgenden Befehl an der Eingabeaufforderung des Computers ein, auf dem der Verwaltungsdienst ausgeführt wird: **net start arssvc**

Untersuchen des Änderungsverlaufs

Auf das Änderungsverlaufsprotokoll können Sie von der ActiveRoles Server-Konsole aus zugreifen. So können Sie schnell untersuchen, welche Änderungen an einem bestimmten Benutzer oder einer bestimmten Gruppen vorgenommen wurden und wer diese wann vorgenommen hat. Wenn beispielsweise ein Kennwort mit Hilfe von ActiveRoles Server zurückgesetzt wurde, können Sie im Änderungsverlauf anzeigen, wer dies getan hat und wann.

Um Änderungen an einem bestimmten Objekt (z.B. an einem Benutzer- oder Gruppenobjekt) zu untersuchen, klicken Sie auf der ActiveRoles Server-Konsole mit der rechten Maustaste auf das Objekt, und klicken Sie dann auf **Änderungsverlauf**. Damit wird ein Fenster angezeigt, das der folgenden Abbildung ähnelt.



Standardmäßig werden im Fenster **Änderungsverlauf** nur grundlegende Optionen angezeigt. Sie können weitere Optionen anzeigen, indem Sie auf das Plus-Zeichen (+) in der oberen linken Ecke neben der ersten Spaltenüberschrift klicken.

Im Fenster **Änderungsverlauf** finden Sie die folgenden Informationen:

- **Name** Der Name des Objekts, für das Sie den Änderungsverlauf untersuchen. Klicken Sie auf die Schaltfläche **Eigenschaften**, um die Eigenschaften des Objekts anzuzeigen oder zu ändern.
- **Abgeschlossen am** Beantwortet die Frage „Wann wurden die Änderungen vorgenommen?"
- **Vorgangszusammenfassung** Beantwortet die Frage „Welche Änderungen wurden vorgenommen?"
- **Angefordert von** Beantwortet die Frage „Wer hat die Änderungen vorgenommen?"

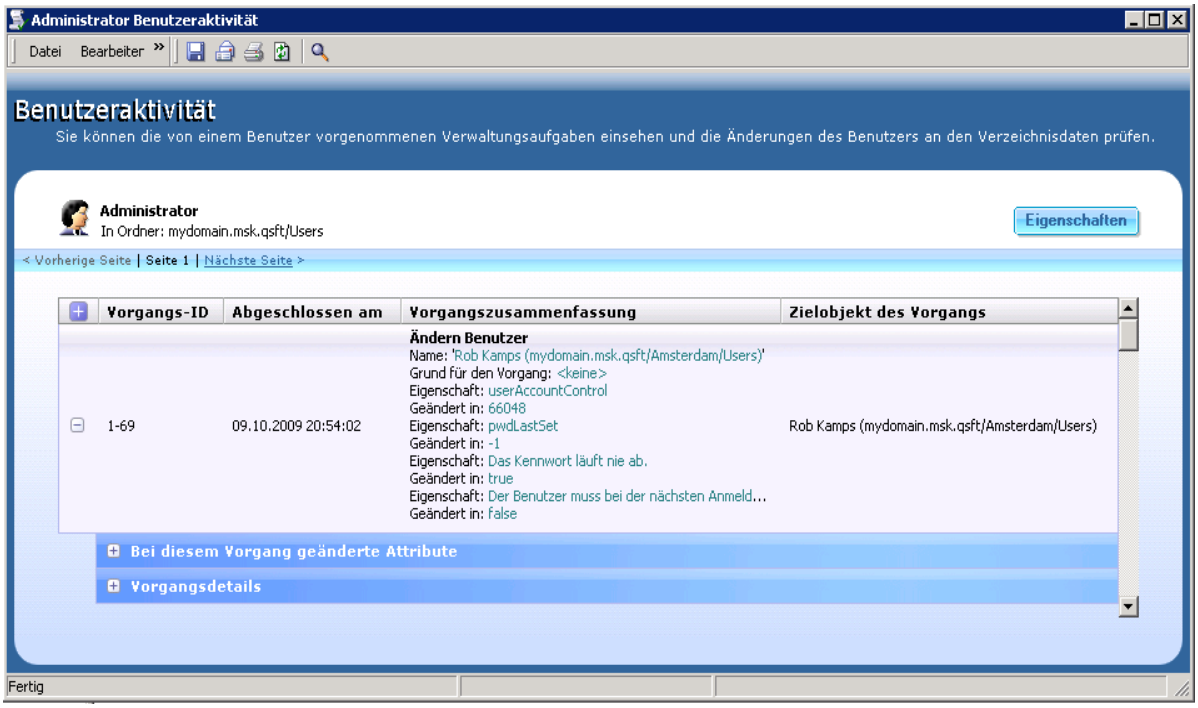
Das Fenster **Änderungsverlauf** umfasst auch die folgenden Bereiche:

- **Bei diesem Vorgang geänderte Attribute** Informationen über die Objektattribute, die geändert wurden, über neue, den Attributen zugeordnete Werte und über das Konto, das verwendet wurde, um die Änderungen vorzunehmen.
- **Vorgangsdetails** Zusätzliche Informationen darüber, wann und von wem die Änderungen angefordert wurden und wer die Änderungen genehmigt hat, wenn irgendeine Genehmigung erforderlich war.

Untersuchen von Benutzeraktivitäten

Im Änderungsverlaufsprotokoll können Sie auch die Änderungen untersuchen, die ein bestimmter Benutzer an Verzeichnisdaten vorgenommen hat, d.h. die Verwaltungsaktivitäten des Benutzers. Die Verwaltungsaktivität-Verweildauer hängt von der Konfiguration des Änderungsverfolgungsprotokolls ab (siehe „Richtlinie für die Änderungsnachverfolgung" weiter oben in diesem Kapitel).

Um anzuzeigen, welche Änderungen ein bestimmter Benutzer vorgenommen hat, klicken Sie auf der ActiveRoles Server-Konsole mit der rechten Maustaste auf das Benutzerobjekt, und klicken Sie dann auf **Benutzeraktivität**. Damit wird ein Fenster angezeigt, das der folgenden Abbildung ähnelt.



Standardmäßig werden im Fenster **Benutzeraktivität** nur grundlegende Optionen angezeigt. Sie können weitere Optionen anzeigen, indem Sie auf das Plus-Zeichen (+) in der oberen linken Ecke neben der ersten Spaltenüberschrift klicken.

Im Fenster **Benutzeraktivität** finden Sie die folgenden Informationen:

- **Name** Der Name des Benutzers, der die von Ihnen untersuchten Änderungen vorgenommen hat.
- **Abgeschlossen am** Datum und Uhrzeit, wann die Änderungen vorgenommen wurden.
- **Vorgangszusammenfassung** Eine Beschreibung der Änderungen, die an dem Objekt vorgenommen wurden.
- **Zielobjekt des Vorgangs** Der Name des Objekts, an dem die Änderungen vorgenommen wurden.

Das Fenster enthält außerdem die gleichen zusätzlichen Abschnitte wie das Fenster **Änderungsverlauf**.

13

Papierkorb

- Beschreibung der Papierkorbfunktion
- Suchen und Auflisten gelöschter Objekte
- Wiederherstellen eines gelöschten Objekts
- Delegieren von Vorgängen an gelöschten Objekten
- Anwenden von Richtlinien- oder Arbeitsablaufregeln

Beschreibung der Papierkorbfunktion

ActiveRoles Server stützt sich auf den Active Directory-Papierkorb, eine in Microsoft Windows Server 2008 R2 eingeführte Funktion der Active Directory-Domänendienste, um die Wiederherstellung von gelöschten Objekten zu erleichtern. Wenn der Papierkorb aktiviert ist, kann in ActiveRoles Server auf einfache Weise ein versehentlicher Löschvorgang rückgängig gemacht werden. Dies verringert die im Zusammenhang mit der Wiederherstellung von gelöschten Objekten in Active Directory aufgewandte Zeit, die Kosten und die Auswirkungen auf die Benutzer.

Die Verwendung von ActiveRoles Server in Verbindung mit der Active Directory-Papierkorbfunktion trägt zur Minimierung der Ausfallzeiten des Verzeichnisdienstes durch versehentliches Löschen von Verzeichnisdaten bei. Der Papierkorb bietet die Möglichkeit, gelöschte Objekte ohne Zuhilfenahme von Sicherungen oder den Neustart von Domänencontrollern wiederherzustellen. Eine von ActiveRoles Server bereitgestellte Benutzerschnittstelle beschleunigt das Auffinden und die Wiederherstellung von gelöschten Objekten aus dem Papierkorb. Die flexiblen und leistungsfähigen, von ActiveRoles Server für die Delegation von Verwaltungsaufgaben, die Erzwingung von Richtlinienregeln und Genehmigungen und die Verfolgung von Änderungen bereitgestellten Mechanismen gewährleisten eine engmaschige Kontrolle des Wiederherstellungsprozesses.

Um Löschvorgänge rückgängig zu machen, stützt sich ActiveRoles Server auf die Möglichkeit des Active Directory-Papierkorbs, alle Attribute einschließlich der mit Verknüpfungen verbundenen Attribute der gelöschten Objekte beizubehalten. Hierdurch ist es möglich, gelöschte Objekte in den Status zurückzuversetzen, in dem sie sich unmittelbar vor dem Löschvorgang befunden haben. So erhalten zum Beispiel wiederhergestellte Benutzerkonten alle Gruppenmitgliedschaften zurück, die sie vor dem Löschvorgang besessen haben.

ActiveRoles Server kann verwendet werden, um gelöschte Objekte in jeder beliebigen verwalteten Domäne wiederherzustellen, in der die Active Directory-Papierkorbfunktion aktiviert ist. Dies erfordert die Gesamtstruktur-Funktionsebene von Windows Server 2008 R2, sodass alle Gesamtstruktur-Domänen-controller Windows Server 2008 R2 ausführen müssen. In einer Gesamtstruktur, die diese Voraussetzungen erfüllt, kann ein Administrator den Papierkorb mit Hilfe des Active Directory-Moduls für Windows PowerShell in Windows Server 2008 R2 aktivieren. Weitere Informationen über den Active Directory-Papierkorb finden Sie unter Neues in AD DS: Active Directory-Papierkorb (http://go.microsoft.com/fwlink/?LinkId=141392).

Suchen und Auflisten gelöschter Objekte

Wenn der Active Directory-Papierkorb in einer verwalteten Domäne aktiviert ist, ermöglicht ActiveRoles Server den Zugriff auf den Container **Gelöschte Objekte**, der die gelöschten Objekte aus dieser Domäne enthält. In der ActiveRoles Server-Konsolenstruktur wird der Container auf derselben Ebene wie die Domäne selbst unter dem Knoten **Active Directory** angezeigt. Wenn für mehrere verwaltete Domänen der Active Directory-Papierkorb aktiviert ist, dann wird ein separater Container für jede Domäne angezeigt. Um die Container voneinander unterscheiden zu können, enthält der Name des Containers den Domänennamen (zum Beispiel, **MeineDomäne.MeinComputer.com – Gelöschte Objekte**).

Suchseiten in der ActiveRoles Server-Konsole erleichtern das Auffinden gelöschter Objekte und die Aktivierung der Verwendung sehr spezifischer Abfragen, die auf beliebigen Objekteigenschaften beruhen. Es ist außerdem möglich, eine Liste der gelöschten Objekte, die sich zum Zeitpunkt des Löschvorgangs in einer bestimmten Organisationseinheit oder verwalteten Einheit befunden haben, zu untersuchen und zu durchsuchen.

Suchen nach dem Container „Gelöschte Objekte"

Die ActiveRoles Server-Konsole enthält die Suchkategorie **Gelöschte Objekte** im Dialogfeld **Suchen**, die zur Durchführung einer Suche im Container **Gelöschte Objekte** jeder beliebigen verwalteten Domäne dient, in der der Active Directory-Papierkorb aktiviert ist.

Gehen Sie folgendermaßen vor, um nach dem Container „Gelöschte Objekte" zu suchen:

1. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf den Container **Gelöschte Objekte** und klicken Sie dann auf **Suchen**.
2. Führen Sie einen der nachfolgend aufgeführten Schritte aus:
   - Geben Sie im Feld **Name** oder **Beschreibung** den Namen bzw. die Beschreibung oder einen Teil des Namens oder der Beschreibung des zu suchenden Objekts ein.

     *Bei der Suche nach Namen verwendet ActiveRoles Server die Ambiguous Name Resolution (ANR), um Objekte zu finden, deren Name, aber auch andere Eigenschaften mit der von Ihnen im Feld **Name** eingegebenen Zeichenfolge übereinstimmen. Die für ANR verwendeten Eigenschaften umfassen den Namen, den Vornamen, den Nachnamen, den Anzeigenamen und den Anmeldenamen.*

   - Klicken Sie auf die Schaltfläche neben dem Feld **Gelöscht aus** und wählen Sie das Objekt aus, bei dem es sich um das übergeordnete Objekt des zu suchenden, gelöschten Objekts handelt.

     *Mit der Suchoption **Gelöscht aus** können Sie nach untergeordneten Objekten suchen, die aus einem bestimmten Containerobjekt gelöscht wurden.*

   - Verwenden Sie die Registerkarte **Erweitert**, um eine Abfrage auf der Grundlage von anderen Eigenschaften des zu suchenden gelöschten Objekts zu erstellen. Schrittweise Anleitungen finden Sie unter „Verwenden von erweiterten Optionen für die Suche" in der ActiveRoles Server-Hilfe.
3. Klicken Sie auf **Jetzt suchen**, um die Suchen zu starten.

Nach Abschluss der Suche wird im Dialogfeld **Suchen** eine Liste der mit den Suchkriterien übereinstimmenden gelöschten Objekte angezeigt.

Wenn Sie auf ein Objekt in der Liste der Suchergebnisse doppelklicken, werden die Eigenschaftenseiten für dieses Objekt angezeigt. Wenn Sie mit der rechten Maustaste auf ein Objekt klicken, werden im Kontextmenü alle Aktionen angezeigt, die Sie an diesem Objekt durchführen können.

Suchen nach Objekten, die aus einer bestimmten Organisationseinheit oder verwalteten Einheit gelöscht wurden

Um eine Liste der Objekte anzuzeigen und zu durchsuchen, die aus einer bestimmten Organisationseinheit oder verwalteten Einheit gelöscht wurden, können Sie den Befehl **Gelöschte Objekte anzeigen oder wiederherstellen** verwenden. Der Befehl öffnet ein Dialogfeld, in dem die gelöschten Objekte aufgeführt sind, die der entsprechenden Organisationseinheit oder verwalteten Einheit zum Zeitpunkt des Löschvorgangs direkt untergeordnet waren. Das Dialogfeld **Gelöschte Objekte anzeigen oder wiederherstellen** kann für die Suche nach gelöschten Objekten verwendet werden, deren Name mit einer bestimmten Suchzeichenkette übereinstimmt. Es bietet eine flexible Übereinstimmung, da es die mehrdeutige Namensauflösung (Ambiguous Name Resolution, ANR) unterstützt.

Gehen Sie folgendermaßen vor, um nach Objekten zu suchen, die aus einer bestimmten Organisationseinheit oder verwalteten Einheit gelöscht wurden:

1. Klicken Sie mit der rechten Maustaste auf die Organisationseinheit oder verwaltete Einheit und klicken Sie dann auf **Gelöschte Objekte anzeigen oder wiederherstellen**.
2. Geben Sie im Feld **Suchen nach** die Suchzeichenkette ein, die Sie verwenden möchten.
3. Klicken Sie auf **Jetzt suchen**, um die Suchen zu starten.

Wenn die Suche abgeschlossen ist, ist die Liste im Dialogfeld auf die gelöschten Objekte beschränkt, deren Name, Vorname, Nachname, Anzeigename, Anmeldename oder jegliche andere für ANR verwendete Eigenschaft mit der angegebenen Suchzeichenkette beginnt. Um die Suchergebnisse zu löschen und alle gelöschten Objekte anzuzeigen, klicken Sie auf die Schaltfläche **Suche löschen**.

Der Befehl **Gelöschte Objekte anzeigen oder wiederherstellen** ist auch für Domänen- und Containerobjekte verfügbar. Somit können Sie auch nach gelöschten Objekten suchen, die zum Zeitpunkt des Löschvorgangs einer bestimmten Domäne oder einem bestimmten Container direkt untergeordnet waren.

Wiederherstellen eines gelöschten Objekts

Für die Wiederherstellung von gelöschten Objekten können Sie den Befehl **Wiederherstellen** verwenden, der in folgenden Elementen verfügbar ist:

- Im Dialogfeld **Gelöschte Objekte anzeigen oder wiederherstellen**
- In einer Liste der Suchergebnisse, die mit Hilfe der Suchkategorie **Gelöschte Objekte** im Dialogfeld **Suchen** vorbereitet wird
- In einer Liste der Objekte, die sich im Container **Gelöschte Objekte** befinden; diese Liste wird im Bereich „Details" angezeigt, wenn Sie den Container **Gelöschte Objekte** in der Konsolenstruktur auswählen

In der ActiveRoles Server-Konsole befindet sich der Befehl im Kontextmenü, das angezeigt wird, wenn Sie mit der rechten Maustaste auf ein gelöschtes Objekt klicken.

Gehen Sie folgendermaßen vor, um ein gelöschtes Objekt wiederherzustellen:

1. Klicken Sie im Dialogfeld **Gelöschte Objekte anzeigen oder wiederherstellen** auf das gelöschte Objekt und klicken Sie dann auf die Schaltfläche **Wiederherstellen**.

   – ODER –

   Klicken Sie in einer Liste der Suchergebnisse, die mit Hilfe der Suchkategorie **Gelöschte Objekte** vorbereitet wurde, oder in einer Liste der Objekte, die sich im Container **Gelöschte Objekte** befinden, mit der rechten Maustaste auf das gelöschte Objekt und dann auf **Wiederherstellen**.

2. Überprüfen und ändern Sie bei Bedarf die Einstellungen im Dialogfeld **Objekt wiederherstellen** und klicken Sie dann auf **OK**, um den Wiederherstellunsvorgang zu starten.

Im Dialogfeld **Objekt wiederherstellen** werden Sie aufgefordert, festzulegen, ob gelöschte untergeordnete Objekte des gelöschten Objekts ebenfalls wiederhergestellt werden sollen. Das Kontrollkästchen **Untergeordnete Objekte wiederherstellen** ist standardmäßig aktiviert. Dies gewährleistet, dass der auf ein gelöschtes Containerobjekt angewandte Befehl **Wiederherstellen** den gesamten Inhalt des Containers wiederherstellt.

Betrachten Sie zur Veranschaulichung das Beispiel, in dem ein Administrator versehentlich die Organisationseinheit mit dem Namen „Sales_Department", die eine Reihe von Benutzerkonten für das Vertriebspersonal enthält, gemeinsam mit einer anderen Organisationseinheit mit der Bezeichnung „Admins", die ihrerseits ein Benutzerkonto für einen administrativen Assistenten enthält, löscht. Bei Anwendung des Befehls **Wiederherstellen** auf die Organisationseinheit „Sales_Department" mit der Option zur Wiederherstellung von untergeordneten Objekten führt ActiveRoles Server die folgenden Schritte aus:

1. Wiederherstellung der Organisationseinheit „Sales_Department"
2. Wiederherstellung aller gelöschten Benutzerkonten, die der Organisationseinheit „Sales_Department" direkt untergeordnet waren
3. Wiederherstellung der Organisationseinheit „Admins" in der Organisationseinheit „Sales_Department"
4. Wiederherstellung aller gelöschten Benutzerkonten, die der Organisationseinheit „Admins" direkt untergeordnet waren

Wenn Sie das Kontrollkästchen **Untergeordnete Objekte wiederherstellen** deaktivieren, führt ActiveRoles Server nur den ersten Schritt durch, sodass die wiederhergestellte Organisationseinheit „Sales_Department" leer ist.

Stellen Sie bei der Wiederherstellung eines gelöschten Objekts sicher, dass sein übergeordnetes Objekt nicht gelöscht wird. Das übergeordnete Objekt können Sie durch Anzeige der Eigenschaften des gelöschten Objekts ermitteln: Der kanonische Name des übergeordneten Objekts, dem die Bezeichnung „gelöscht aus:" voransteht, wird neben dem Namen des gelöschten Objekts auf der Registerkarte **Allgemein** im Dialogfeld **Eigenschaften** angezeigt. Wenn das übergeordnete Objekt gelöscht ist, müssen Sie es wiederherstellen, bevor Sie dessen untergeordnete Objekte wiederherstellen, da gelöschte Objekte in einem aktiven übergeordneten Objekt wiederhergestellt werden müssen.

Delegieren von Vorgängen an gelöschten Objekten

Das auf den ActiveRoles Server-Zugriffsvorlagen basierende Delegationsmodell lässt sich vollständig auf die für die gelöschten Objekte spezifischen Verwaltungsaufgaben übertragen. Eine neue Zugriffsvorlage mit der Bezeichnung **Alle Objekte – Gelöschte Objekte anzeigen oder wiederherstellen** erleichtert die Delegation der folgenden Vorgänge an ausgewählten Benutzer:

- Anzeigen gelöschter Active Directory-Objekte
- Wiederherstellen eines gelöschten Active Directory-Objekts

Bei Anwendung auf den Container **Gelöschte Objekte** verleiht die Zugriffsvorlage den delegierten Benutzern das Recht, jedes beliebige gelöschte Objekt anzuzeigen und wiederherzustellen. Bei Anwendung der Zugriffsvorlage auf eine Organisationseinheit oder eine verwaltete Einheit erhalten die delegierten Benutzer das Recht, nur die gelöschten Objekte anzuzeigen und wiederherzustellen, die sich zum Zeitpunkt des Löschvorgangs in dieser Organisationseinheit oder verwalteten Einheit befunden haben.

Gehen Sie folgendermaßen vor, um den Vorgang der Wiederherstellung gelöschter Objekte zu delegieren:

1. Wählen Sie in der Konsolenstruktur **Configuration | Access Templates | Active Directory**.
2. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf **Alle Objekte – Gelöschte Objekte anzeigen oder wiederherstellen** und klicken Sie dann auf **Verknüpfungen**.
3. Klicken Sie im Dialogfeld **Verknüpfungen** auf **Hinzufügen**.
4. Klicken Sie auf der Begrüßungsseite im Assistenten zum Delegieren der Kontrolle auf **Weiter**.
5. Klicken Sie auf der Seite **Objekte** im Assistenten auf **Hinzufügen**; wählen Sie dann den Container aus, in dem Sie den Vorgang der Wiederherstellung von gelöschten Objekten delegieren möchten:
   - Um die Wiederherstellung nur von den gelöschten Objekte zu delegieren, die sich zum Zeitpunkt des Löschvorgangs in einer bestimmten Organisationseinheit oder verwalteten Einheit befunden haben, wählen Sie die Organisationseinheit oder verwaltete Einheit aus.
   - Um die Wiederherstellung jedes beliebigen gelöschten Objeks in einer bestimmten verwalteten Domäne zu delegieren, wählen Sie entweder das Objekt, das diese Domäne angibt, oder den Container **Gelöschte Objekte** für diese Domäne aus.
   - Um die Wiederherstellung jedes beliebigen gelöschten Objekts in jeder beliebigen verwalteten Domäne zu delegieren, wählen Sie den Container **Active Directory** aus.
6. Befolgen Sie die Anweisungen des Assistenten, um den Assistenten zum Delegieren der Kontrolle abzuschließen.
7. Klicken Sie auf **OK**, um das Dialogfeld **Verknüpfungen** zu schließen.

Obwohl es möglich ist, den Vorgang der Wiederherstellung gelöschter Objekte in jeder beliebigen verwalteten Domäne, Organisationseinheit oder verwalteten Einheit zu delegieren, kann ein gelöschtes Objekt nur dann mit Hilfe von ActiveRoles Server wiederhergestellt werden, wenn das Objekt zu einer verwalteten Domäne gehört, in der die Active Directory-Papierkorbfunktion aktiviert ist. Anweisungen bezüglich der Aktivierung des Papierkorbs finden Sie unter „Active Directory-Papierkorb – Schrittweise Anleitung" in der Dokumentation zu Windows Server 2008 R2 von Microsoft.

Anwenden von Richtlinien- oder Arbeitsablaufregeln

Zusätzlich zur Delegation von Verwaltungsaufgaben bietet ActiveRoles Server die Möglichkeit, eine richtlinienbasierte Kontrolle über den Vorgang der Wiederherstellung gelöschter Objekte zu erstellen. Richtlinienregeln können verwendet werden, um zusätzliche Überprüfung oder benutzerdefinierte skriptbasierte Vorgänge bei der Wiederherstellung von gelöschten Objekten durchzuführen. Es können Arbeitsablaufregeln angewandt werden, die die Genehmigung für den Wiederherstellungsvorgang oder eine Benachrichtigung per E-Mail über den Abschluss des Wiederherstellungsvorgangs erfordern.

Die Richtlinien- oder Arbeitsablaufregeln für die Kontrolle des Wiederherstellungsvorgangs oder für die sonstige Verwaltung gelöschter Objekte kann in folgenden Elementen definiert werden:

- Der Knoten **Active Directory** in der ActiveRoles Server-Konsole – Die auf diese Weise definierten Regeln betreffen alle gelöschten Objekte in jeder verwalteten Domäne, in der der ActiveRoles Server-Papierkorb aktiviert ist.
- Der Knoten, der eine Domäne oder den Container **Gelöschte Objekte** für diese Domäne in der ActiveRoles Server-Konsole darstellt – Diese Regeln betreffen alle gelöschten Objekte nur in dieser Domäne.
- Eine Organisationseinheit oder verwaltete Einheit, die das Objekt zum Zeitpunkt des Löschvorgangs enthielt – Obwohl das gelöschte Objekt nicht mehr zu dieser Organisationseinheit oder verwalteten Einheit gehört, berücksichtigt ActiveRoles Server den ehemaligen Speicherort des Objekts, sodass die auf diesen Speicherort angewandten Regeln nach dem Löschen auch weiterhin das Objekt betreffen.

Ein Administrator kann zum Beispiel einen Arbeitsablauf so konfigurieren, dass eine Genehmigung für die Wiederherstellung eines jeden Benutzerkontos erforderlich ist, das aus einer bestimmten Organisationseinheit gelöscht wurde. Die Arbeitsablaufdefinition enthält in diesem Fall eine entsprechende Genehmigungsregel und gibt diese Organisationseinheit als den Zielcontainer in den Arbeitsablauf-Startbedingungen an.

Richtlinienregeln werden per Konfiguration und Anwendung von Richtlinienobjekten definiert.

So wenden Sie ein Richtlinienobjekt auf den Container „Gelöschte Objekte" an:

1. Klicken Sie mit der rechten Maustaste auf den Container **Gelöschte Objekte** und klicken Sie dann auf **Richtlinie erzwingen**.
2. Klicken Sie im Dialogfeld **ActiveRoles Server-Richtlinie** auf **Hinzufügen**.
3. Aktivieren Sie im Dialogfeld **Richtlinienobjekte wählen** das Kontrollkästchen neben dem Richtlinienobjekt, das Sie anwenden möchten, und klicken Sie dann auf **OK**.
4. Klicken Sie auf **OK**, um das Dialogfeld **ActiveRoles Serverrichtlinie** zu schließen.

Weitere Informationen und Anweisungen bezüglich der Konfiguration und Anwendung von Richtlinienobjekten finden Sie unter „Verwalten von Richtlinienobjekten" in der ActiveRoles Server-Hilfe.

Arbeitsablaufregeln werden durch Konfiguration von Arbeitsablaufdefinitionen und Festlegung der entsprechenden Arbeitsablauf-Startbedingungen definiert.

Gehen Sie folgendermaßen vor, um einen Arbeitsablauf auf den Container „Gelöschte Objekte" anzuwenden:

1. Wählen Sie in der Konsolenstruktur den Arbeitsablauf aus, den Sie anwenden möchten.

   *Um einen Arbeitsablauf auszuwählen, erweitern Sie **Configuration | Policies | Workflow** und klicken Sie dann auf das Arbeitsablaufdefinitionsobjekt unter **Workflow** in der Konsolenstruktur.*

2. Klicken Sie im Bereich „Details" auf die Verknüpfung über dem Arbeitsablauf-Prozessdiagramm.

   *Daraufhin wird das Dialogfeld **Arbeitsablauf-Startbedingungen** angezeigt.*

3. Klicken Sie auf **Vorgang auswählen**, wählen Sie die Option **Wiederherstellen** und klicken Sie dann auf **Fertig stellen**.

   Hierdurch wird der Arbeitsablauf bei einer Anforderung zur Wiederherstellung eines gelöschten Objekts des angegebenen Typs gestartet.

4. Klicken Sie unter **Initiator-Bedingungen** auf **Hinzufügen**.
5. Klicken Sie auf der Seite **Initiatorbedingung hinzufügen** auf **Durchsuchen** und wählen Sie dann den Container **Gelöschte Objekte**.

   *Sie müssen einen anderen Container als **Gelöschte Objekte** auswählen. Wenn Sie dies tun, startet der Arbeitsablauf nur bei der Wiederherstellung eines Objekts, das aus dem von Ihnen ausgewählten Container gelöscht wurde.*

6. Schließen Sie die Konfiguration der Arbeitsablauf-Startbedingungen ab.

Weitere Informationen über Arbeitsabläufe finden Sie im Kapitel „Arbeitsabläufe" im ActiveRoles Server Administratorhandbuch oder unter dem Thema „Arbeitsablaufkonzepte" in der ActiveRoles Server-Hilfe.

14

AD LDS-Datenverwaltung

- Registrieren einer AD LDS-Instanz
- Verwalten von AD LDS-Objekten
- Anpassen der Konfiguration von ActiveRoles Server

Eine ActiveRoles Server-Lizenz ermöglicht normalerweise nicht die AD LDS-Datenverwaltung. Damit ActiveRoles Server AD LDS-Datenverwaltungsaufgaben durchführen kann, ist eine separate Lizenz erforderlich.

Registrieren einer AD LDS-Instanz

ActiveRoles Server bietet die Möglichkeit, Verzeichnisdaten in Microsoft Active Directory Lightweight Directory Services (AD LDS), einem unabhängigen Modus von Active Directory, zuvor bekannt unter der Bezeichnung „Active Directory Application Mode" (ADAM), zu verwalten.

Eine laufende Kopie des AD LDS Verzeichnisdiensts wird als eine Dienstinstanz (oder einfach *Instanz*) bezeichnet. Um ActiveRoles Server für die Verwaltung von Daten zu verwenden, die vom AD LDS Verzeichnisdienst gehostet werden, müssen Sie zunächst die Instanz registrieren, in der sich die zu verwaltenden Daten befinden.

Wenn eine Instanz registriert wurde, können die ActiveRoles Server Client-Schnittstellen – Konsole, Web-Interface und ADSI Provider – verwendet werden, um die Verzeichnisdaten in den in der Instanz gefundenen Anwendungs- und Konfigurationspartitionen aufzurufen, anzuzeigen und zu ändern. Die bei ActiveRoles Server registrierten Instanzen werden als *verwaltete AD LDS-Instanzen* bezeichnet.

Gehen Sie folgendermaßen vor, um eine AD LDS-Instanz bei ActiveRoles Server zu registrieren:

1. Öffnen Sie die ActiveRoles Server-Konsole.
2. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration | Server configuration**, klicken Sie mit der rechten Maustaste auf **Managed AD LDS Instances (ADAM)** und wählen Sie **Neu | Verwaltete AD LDS-Instanz (ADAM)**, um den Assistenten für verwaltete AD LDS-Instanz hinzufügen zu starten.
3. Folgen Sie den Anweisungen des Assistenten.
4. Geben Sie auf der Seite **Zu registrierende AD LDS-Instanz** den Servernamen und die Anschlussnummer der AD LDS-Instanz an, die Sie bei ActiveRoles Server registrieren möchten.

   Geben Sie unter **Server** den vollqualifizierten DNS-Namen (zum Beispiel server.company.com) des Computers an, auf dem die Instanz ausgeführt wird. Geben Sie unter **LDAP-Anschluss** die Nummer des Lightweight Directory Access Protocol (LDAP) Kommunikationsanschlusses an, der von der Instanz verwendet wird (der Standard-Kommunikationsanschluss für LDAP ist 389). Sie können auch auf **Auswählen** klicken, um die AD LDS-Instanz, die Sie registrieren möchten, zu suchen und auszuwählen.

5. Geben Sie auf der Seite **ActiveRoles Server-Anmeldeinformationen** die Anmelde-informationen an, die ActiveRoles Server für den Zugriff auf die Instanz verwenden wird.

   Wenn Sie möchten, dass jeder Verwaltungsdienst im Sicherheitskontext seines eigenen Dienstkonto die Verbindung zur Instanz herstellt, dann klicken Sie auf **Die Dienstkontoinformationen, die der Verwaltungsdienst zur Anmeldung verwendet**. Bei Auswahl dieser Option können verschiedene Verwaltungsdienste unterschiedliche Zugriffsebenen auf die Instanz haben (das Dienstkonto eines Dienstes kann administrative Zugriffsrechte auf die Instanz haben, während das Dienstkonto eines anderen Dienstes nicht über diese Rechte verfügt). Folglich kann der Wechsel von einem Verwaltungsdienst zum anderen dazu führen, dass ActiveRoles Server den Zugriff auf die Instanz verliert.

   Wenn Sie möchten, dass jeder Verwaltungsdienst mit Hilfe desselben Benutzerkontos eine Verbindung zur Instanz aufbaut, dann klicken Sie auf **Die unten angegebenen Windows Benutzerkontoinformationen** und geben Sie den Benutzernamen, das Kennwort und den Domänennamen ein. Auf diese Weise geben Sie ein so genanntes *Vorrangiges Konto* an, wodurch die Zugriffsrechte von ActiveRoles Server auf die Instanz von den Zugriffsrechten dieses Benutzerkontos bestimmt werden (anstatt von den Zugriffsrechten des Dienstkontos des Verwaltungsdienstes).

6. Klicken Sie auf der Abschlussseite auf **Fertig stellen**, um den Registrierungsvorgang zu starten.

Das von Ihnen in Schritt 5 angegebene vorrangige Konto muss über die vollständige administrative Kontrolle über diese Instanz verfügen. D. h. es muss ein Mitglied der Administratorengruppe in der Konfigurationsverzeichnispartition der Instanz sein. Wenn Sie sich dazu entschließen, kein vorrangiges Konto anzugeben, dann müssen Sie sicherstellen, dass das Dienstkonto jeder Ihrer Verwaltungsdienste dieser Anforderung entspricht. Verwenden Sie das ADAM ADSI Edit Snap-in, um das vorrangige Konto oder das Dienstkonto zur Administratorengruppe in der Konfigurationsverzeichnispartition hinzuzufügen, bevor Sie die Instanz bei ActiveRoles Server registrieren.

Nach der Registrierung einer AD LDS (ADAM) -Instanz können Sie ihre Registrierungseinstellungen anzeigen oder ändern, indem Sie den Befehl **Eigenschaften** für das Objekt ausführen, das diese Instanz im Container **Managed AD LDS Instances (ADAM)** repräsentiert. Dann können Sie Änderungen an den in Schritt 5 oben ausgewählten Optionen vornehmen.

Wenn Sie eine AD LDS (ADAM) -Instanz nicht mehr mit ActiveRoles Server verwalten möchten, können Sie die Registrierung der Instanz aufheben, indem Sie den Befehl **Löschen** für das Objekt ausführen, das diese Instanz im Container **Managed AD LDS Instances (ADAM)** repräsentiert. Durch die Aufhebung der Registrierung einer Instanz werden nur die Registrierungsinformationen von ActiveRoles Server entfernt. Es werden keine Änderungen an den von dieser Instanz gehosteten Verzeichnisdaten vorgenommen.

Verwalten von AD LDS-Objekten

Die in den verwalteten AD LDS-Instanzen gefundenen Anwendungs- und Konfigurationspartitionen werden in einem Container der obersten Ebene zusammengefasst, was das Auffinden der AD LDS-Daten erleichtert. Jede Partition wird durch einen separaten Container (Knoten) dargestellt, sodass Sie die Partitionsstruktur auf gleiche Weise durchblättern können, wie Sie dies für eine Active Directory-Domäne tun.

Die ActiveRoles Server-Konsole unterstützt eine Vielzahl von administrativen Vorgängen an AD LDS-Benutzern, -Gruppen und anderen Objekten. Sie können Verzeichnisobjekte wie etwa Benutzer, Gruppen, Container und Organisationseinheiten in den verwalteten AD LDS-Instanzen auf gleiche Weise erstellen, anzeigen, ändern und löschen, wie Sie dies für Verzeichnisobjekte in Active Directory-Domänen tun.

Gehen Sie folgendermaßen vor, um die Verzeichnisstruktur zu durchzublättern und um AD LDS-Objekte zu verwalten:

1. Doppelklicken Sie in der Konsolenstruktur unter dem Stammverzeichnis der Konsolenstruktur auf den Container **AD LDS (ADAM)**.
2. Doppelklicken Sie in der Konsolenstruktur unter **AD LDS (ADAM)** auf ein Verzeichnispartitionsobjekt, um dessen Container der obersten Ebene anzuzeigen.
3. Doppelklicken Sie in der Konsolenstruktur auf einen Container der obersten Ebene, um die nächste Objektebene in diesem Container anzuzeigen.
4. Führen Sie eine der folgenden Aktionen durch:
   - Um die nächst tiefere Verzweigung der Verzeichnisstruktur anzuzeigen, doppelklicken Sie auf die nächst tiefere Containerebene in der Konsolenstruktur.
   - Um ein Verzeichnisobjekt auf der aktuellen Verzeichnisebene zu verwalten, klicken Sie mit der rechten Maustaste auf das Verzeichnisobjekt im Bereich „Details" und verwenden Sie die Befehle im Kontextmenü.

Im Container **AD LDS (ADAM)** ist jede Verzeichnispartition durch eine Bezeichnung gekennzeichnet, die sich aus dem Namen der Partition, dem DNS-Namen des Computers, auf dem die AD LDS-Instanz ausgeführt wird, die die Partition hostet, und der Nummer des von der Instanz verwendeten LDAP-Anschlusses zusammensetzt.

Normalerweise zeigt die Konsole nur die Anwendungsverzeichnispartitionen an. Um die Konfigurations- oder Schemapartition anzuzeigen, wechseln Sie in den Rohansichtsmodus: Wählen Sie **Ansicht | Modus**, klicken Sie auf **Rohmodus** und klicken Sie dann auf **OK**.

Sie können nur die Datenverwaltungsaufgaben ausführen, denen Sie in ActiveRoles Server zugeordnet sind. Daher werden nur die Befehle, die Sie verwenden dürfen, und die Objekte, die Sie anzeigen oder ändern dürfen, angezeigt.

Zusätzlich zur Zugriffskontrolle ermöglicht ActiveRoles Server die Richtlinienumsetzung für Verzeichnisdaten. Richtlinien können den Zugriff auf bestimmte Teile der Verzeichnisobjekte einschränken, was zur Folge hat, dass Dateneinträge auf eine Auswahl von Optionen beschränkt wird, dass Daten automatisch generiert werden und es keine Möglichkeit zur Änderung der Daten gibt oder dass die Eingabe von Daten erforderlich ist. Die Konsole bietet eine visuelle Markierung der Dateneinträge, die durch Richtlinien kontrolliert werden: Die Bezeichnungen derartiger Dateneinträge sind in den Dialogfeldern unterstrichen, sodass der Benutzer Richtlinieneinschränkungen untersuchen kann, indem er auf eine Bezeichnung klickt.

Hinzufügen eines AD LDS-Benutzers zum Verzeichnis

Um die Erstellung von Benutzern in AD LDS zu ermöglichen, muss der Administrator zunächst die optionalen Definitionen der von AD LDS bereitgestellten Benutzerobjektklassen importieren. Diese Definitionen sind in importfähigen .ldf-Dateien (ms-User.ldf, ms-InetOrgPerson.ldf, ms-UserProxy.ldf), die sich auf dem Computer befinden, der die AD LDS-Instanz ausführt. Alternativ können die Softwareentwickler das AD LDS-Schema um ihre benutzerdefinierten Definitionen von AD LDS-Benutzerobjektklassen erweitern. Details bezüglich der Erweiterung des AD LDS-Schemas finden Sie in der Dokumentation von Microsoft, die im Lieferumfang von AD LDS enthalten ist.

Gehen Sie folgendermaßen vor, um einen AD LDS-Benutzer zum Verzeichnis hinzuzufügen:

1. Klicken Sie in der Konsolenstruktur unter **AD LDS (ADAM)** mit der rechten Maustaste auf den Container, zu dem Sie den Benutzer hinzufügen möchten, und wählen Sie dann **Neu | Benutzer**, um den Assistenten zu starten, der Sie bei der Durchführung der Benutzererstellung unterstützt.
2. Befolgen Sie die Anweisungen des Assistenten, um die Werte für die Benutzereigenschaften festzulegen.
3. Wenn Sie Werte für zusätzliche Eigenschaften festlegen möchten (solche, für die der Assistent keine Dateneingaben vorsieht), klicken Sie auf der letzten Seite des Assistenten auf **Attribute bearbeiten**.
4. Nachdem Sie die Einstellungen für alle zusätzlichen Eigenschaften für den neuen Benutzer festgelegt haben, klicken Sie auf der letzten Seite des Assistenten auf **Fertig stellen**.

Standardmäßig wird ein AD LDS-Benutzer aktiviert, wenn der Benutzer erstellt wird. Wenn Sie jedoch einem neuen AD LDS-Benutzer ein falsches Kennwort zuordnen oder das Kennwort leer lassen, kann das neu erstellte AD LDS-Benutzerkonto deaktiviert werden. Eine unter Windows Server 2003 ausgeführte AD LDS-Instanz erzwingt also automatisch die Anwendung aller vorhandenen lokalen oder Domänen-Kennwortrichtlinien. Wenn Sie einen neuen AD LDS-Benutzer erstellen und diesem Benutzer ein Kennwort zuweisen, das nicht den Anforderungen der gültigen Kennwortrichtlinie entspricht, wird das

neu erstellte Benutzerkonto deaktiviert. Bevor Sie das Benutzerkonto aktivieren können, müssen Sie ein Kennwort für das Konto festlegen, das den Einschränkungen der Kennwortrichtlinie entspricht. Die Anweisungen bezüglich der Festlegung des Kennworts für einen AD LDS-Benutzer und der Aktivierung eines AD LDS-Benutzers sind weiter unten in diesem Abschnitt aufgeführt.

Hinzufügen einer AD LDS-Gruppe zum Verzeichnis

AD LDS bietet Standardgruppen, die sich im Container **Rollen** jeder Verzeichnispartition in AD LDS befinden. Sie können bei Bedarf zusätzliche AD LDS-Gruppen erstellen. Neue Gruppen können in jedem beliebigen Container erstellt werden.

Gehen Sie folgendermaßen vor, um eine AD LDS-Gruppe zum Verzeichnis hinzuzufügen:

1. Klicken Sie in der Konsolenstruktur unter **AD LDS (ADAM)** mit der rechten Maustaste auf den Container, zu dem Sie die Gruppe hinzufügen möchten, und wählen Sie dann **Neu | Gruppe**, um den Assistenten zu starten, der Sie bei der Durchführung der Gruppenerstellung unterstützt.
2. Befolgen Sie die Anweisungen des Assistenten, um die Werte für die Gruppeneigenschaften festzulegen.
3. Wenn Sie Werte für zusätzliche Eigenschaften festlegen möchten (solche, für die der Assistent keine Dateneingaben vorsieht), klicken Sie auf der letzten Seite des Assistenten auf **Attribute bearbeiten**.
4. Nachdem Sie die Einstellungen für alle zusätzlichen Eigenschaften für die neue Gruppe festgelegt haben, klicken Sie auf der letzten Seite des Assistenten auf **Fertig stellen**.

Sie können sowohl AD LDS-Benutzer als auch Windows-Benutzer zu den von Ihnen erstellten AD LDS-Gruppen hinzufügen. Anweisungen finden Sie im folgenden Unterabschnitt.

Hinzufügen oder Entfernen von Mitgliedern zu bzw. aus einer AD LDS-Gruppe

Beim Hinzufügen von Mitgliedern zu einer AD LDS-Gruppe können Sie Sicherheitsprinzipals hinzufügen, die sich in AD LDS-Instanzen oder in Active Directory-Domänen befinden. Beispiele für Sicherheitsprinzipals sind AD LDS-Benutzer und Active Directory-Domänenbenutzer und -gruppen.

1. Gehen Sie folgendermaßen vor, um Mitglieder zu einer AD LDS-Gruppe hinzuzufügen bzw. aus ihr zu entfernen.
2. Wählen Sie in der Konsolenstruktur unter **AD LDS (ADAM)** den Container aus, in dem sich die Gruppe befindet.
3. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf die Gruppe und klicken Sie dann auf **Eigenschaften**.
4. Klicken Sie auf der Registerkarte **Mitglieder** im Dialogfeld **Eigenschaften** auf **Hinzufügen**.
5. Verwenden Sie das Dialogfeld **Objekte auswählen**, um die Sicherheitsprinzipals auszuwählen, die Sie zur Gruppe hinzufügen möchten. Klicken Sie abschließend auf **OK**.
6. Wählen Sie auf der Registerkarte **Mitglieder** die Gruppenmitglieder aus, die Sie aus der Gruppe entfernen möchten, und klicken Sie dann auf **Entfernen**.
7. Nachdem Sie die gewünschten Änderungen an der Gruppe vorgenommen haben, klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften** zu schließen.

Wenn Sie das Dialogfeld „Objekte auswählen" für die Suche eines Sicherheitsprinzipals verwenden, müssen Sie zunächst die AD LDS-Verzeichnispartition oder die Active Directory-Domäne angeben, in der sich der Sicherheitsprinzipal befindet: Klicken Sie auf **Durchsuchen** und wählen Sie die entsprechende Partition oder Domäne aus.

Sie können nur Sicherheitsprinzipals auswählen, die sich in verwalteten AD LDS-Instanzen oder Active Directory-Domänen befinden; d. h., Sie können Sicherheitsprinzipals nur aus den Instanzen und Domänen auswählen, die bei ActiveRoles Server registriert sind.

Deaktivieren oder Aktivieren eines AD LDS-Benutzerkontos

Sie können das Konto eines AD LDS-Benutzers deaktivieren, um zu verhindern, dass sich der Benutzer bei der AD LDS-Instanz Replikation von Verwaltungsverlaufsdaten mit diesem Konto anmeldet.

Gehen Sie folgendermaßen vor, um ein AD LDS-Benutzerkonto zu deaktivieren bzw. zu aktivieren:

1. Wählen Sie in der Konsolenstruktur unter **AD LDS (ADAM)** den Container aus, in dem sich das Benutzerkonto befindet.
2. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf das Benutzerkonto und führen Sie einen der folgenden Schritte durch, um den Status des Kontos zu ändern:
   - Wenn das Benutzerkonto aktiviert ist, klicken Sie auf **Konto deaktivieren**.
   - Wenn das Benutzerkonto deaktiviert ist, klicken Sie auf **Konto aktivieren**.

Wenn der AD LDS-Benutzer, dessen Konto Sie deaktivieren möchten, aktuell bei der AD LDS-Instanz angemeldet ist, muss sich dieser Benutzer abmelden, damit die neuen Einstellungen übernommen werden.

Normalerweise wird ein AD LDS-Benutzer aktiviert, wenn der Benutzer erstellt wird. Wenn das Kennwort eines neuen AD LDS-Benutzer jedoch nicht den Anforderungen der gültigen Kennwortrichtlinie entspricht, wird das neu erstellte Benutzerkonto deaktiviert. Bevor Sie das Benutzerkonto aktivieren können, müssen Sie ein Kennwort für das Konto festlegen, das den Einschränkungen der Kennwortrichtlinie entspricht. Anweisungen finden Sie im folgenden Unterabschnitt.

Festlegen oder Ändern des Kennworts eines AD LDS-Benutzers

Jedem AD LDS Sicherheitsprinzipal wie etwa einem AD LDS-Benutzer muss ein Konto und Kennwort zugeordnet werden, das AD LDS für die Authentifizierung verwendet. Sie können die ActiveRoles Server-Konsole verwenden, um das Kennwort eines AD LDS-Benutzers festzulegen oder zu ändern.

Gehen Sie folgendermaßen vor, um das Kennwort eines AD LDS-Benutzers festzulegen oder zu ändern:

1. Wählen Sie in der Konsolenstruktur unter **AD LDS (ADAM)** den Container aus, der das Benutzerkonto des AD LDS-Benutzers enthält, für den Sie das Kennwort festlegen oder ändern möchten.
2. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf das Benutzerkonto und klicken Sie dann auf **Kennwort zurücksetzen**.

3. Geben Sie im Dialogfeld **Kennwort zurücksetzen** ein Kennwort für den Benutzer in das Feld **Neues Kennwort** ein und geben Sie das Kennwort dann erneut in das Feld **Kennwortbestätigung** ein oder klicken Sie auf die Schaltfläche neben **Neues Kennwort**, um ein Kennwort zu generieren.
4. Klicken Sie auf **OK**, um das Dialogfeld **Kennwort zurücksetzen** zu schließen.

Der AD LDS-Benutzer, für den Sie das Kennwort festlegen oder ändern, muss dieses neue Kennwort beim nächsten Mal verwenden, wenn er sich bei AD LDS anmeldet.

Standardmäßig erzwingt eine unter Windows Server 2003 oder höher ausgeführte AD LDS-Instanz automatisch die Anwendung aller vorhandenen lokalen oder Domänen-Kennwortrichtlinien. Wenn Sie ein Kennwort für einen AD LDS-Benutzer festlegen, das nicht den Anforderungen der gültigen Kennwortrichtlinie entspricht, gibt ActiveRoles Server einen Fehler aus.

Hinzufügen einer Organisationseinheit zum Verzeichnis

Um Ihre AD LDS-Benutzer und Gruppen zu organisieren, können Sie Benutzer und Gruppen in Organisationseinheiten zusammenfassen. In AD LDS sowie in Active Directory oder anderen auf dem Lightweight Directory Access Protocol (LDAP) basierenden Verzeichnissen sind Organisationseinheiten die am häufigsten verwendete Methode, um Benutzer und Gruppen zu organisieren. Um eine Organisationseinheit in AD LDS zu erstellen, können Sie die ActiveRoles Server-Konsole wie nachfolgend beschrieben nutzen.

Gehen Sie folgendermaßen vor, um eine Organisationseinheit zum Verzeichnis hinzuzufügen:

1. Klicken Sie in der Konsolenstruktur unter **AD LDS (ADAM)** mit der rechten Maustaste auf den Container, zu dem Sie die Organisationseinheit hinzufügen möchten, und wählen Sie **Neu | Organisationseinheit**.
2. Geben Sie einen Namen für die neue Organisationseinheit ein, klicken Sie auf **Weiter** und klicken Sie dann auf **Fertig stellen**.

Standardmäßig können Organisationseinheiten nur unter den Objektklassen Organisationseinheit (ou=), Land/Region (c=), Organisation (o=) oder Domänen-DNS (dc=) hinzugefügt werden. Sie können zum Beispiel eine Organisationseinheit zu o=Unternehmen,c=US aber nicht zu cn=Anwendung,o=Unternehmen,c=US hinzufügen. Die Schemadefinition der Objektklasse „Organisationseinheit" kann jedoch geändert werden, um andere Einteilungen zu ermöglichen.

Sie können neue AD LDS-Benutzer und -Gruppen in einer AD LDS-Organisationseinheit erstellen. Wenden Sie dazu den Befehl **Neu | Benutzer** oder **Neu | Gruppe** wie weiter oben in diesem Abschnitt beschrieben auf die Organisationseinheit an.

Sie können einen vorhandenen AD LDS-Benutzer oder eine vorhandene AD LDS-Gruppe in eine Organisationseinheit verschieben. Wenden Sie dazu den Befehl **Verschieben** auf diesen Benutzer oder diese Gruppe in der ActiveRoles Server-Konsole an oder verwenden Sie die Drag & Drop-Funktion der Konsole.

Hinzufügen eines AD LDS (ADAM)-Proxyobjekts (Benutzerproxy)

AD LDS-Proxyobjekte werden in besonderen Fällen verwendet, in denen eine Anwendung eine einfache LDAP-Bindung an AD LDS durchführen kann, aber die Anwendung den AD LDS-Benutzer immer noch mit einem Sicherheitsprinzipal (Benutzerkonto) in Active Directory verknüpfen muss. Ein Prozess, durch den AD LDS eine Bindungsanforderung von einer Anwendung akzeptieren und diese Bindungsanforderung auf der Grundlage des Inhalts eines Proxyobjekts an Active Directory umleiten kann, wird als *Bindungsumleitung* bezeichnet.

Die Bindungsumleitung tritt ein, wenn eine Bindung zu AD LDS mit Hilfe eines Proxyobjekts (Benutzerproxy) versucht wird. Ein Proxyobjekt ist ein Objekt in AD LDS, das ein Benutzerkonto in Active Directory angibt. Jedes Proxyobjekt in AD LDS enthält die Sicherheits-ID (SID) eines Benutzers in Active Directory. Wenn eine Anwendung versucht, eine Bindung zu einem Proxyobjekt herzustellen, nimmt AD LDS die SID, die im Proxyobjekt gespeichert ist, zusammen mit dem Kennwort, das zum Zeitpunkt der Bindung angegeben wurde, und liefert Active Directory die SID und das Kennwort zu Authentifizierungszwecken.

Ein Proxyobjekt in AD LDS stellt ein Active Directory-Benutzerkonto dar; es kann vergrößert werden, um zusätzliche Daten zu speichern, die in Zusammenhang mit dem anwendungsspezifischen Benutzerkonto stehen. Durch die Bindungsumleitung können Anwendungen den Identitätsspeicher von Active Directory nutzen und gleichzeitig die Flexibilität der Verwendung von AD LDS als einen Anwendungsdatenspeicher beibehalten.

Gehen Sie folgendermaßen vor, um ein Proxyobjekt zu AD LDS hinzuzufügen:

1. Erweitern Sie in der Konsolenstruktur den Container **AD LDS (ADAM)**.
2. Erweitern Sie in der Konsolenstruktur unter **AD LDS (ADAM)** die Verzeichnispartition, zu der Sie ein Proxyobjekt hinzufügen möchten, und suchen Sie den Container, zu dem Sie das Proxyobjekt hinzufügen möchten.
3. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf den Container, zu dem Sie das Proxyobjekt hinzufügen möchten, und wählen Sie **Neu | Proxy-Objekt**, um den Assistenten zu starten, der Sie bei der Erstellung eines Proxyobjekts unterstützt.
4. Geben Sie einen Namen für das Proxyobjekt ein. Klicken Sie dann auf **Weiter**.
5. Klicken Sie auf **Auswählen** und wählen Sie das Active Directory-Domänen-Benutzerkonto, das durch das Proxyobjekt angegeben werden soll. Klicken Sie dann auf **Weiter**.
6. Wenn Sie Werte für zusätzliche Eigenschaften festlegen möchten (solche, für die der Assistent keine Dateneingaben vorsieht), klicken Sie auf der letzten Seite des Assistenten auf **Attribute bearbeiten**.
7. Nachdem Sie die Einstellungen für alle zusätzlichen Eigenschaften für das neue Objekt festgelegt haben, klicken Sie auf der letzten Seite des Assistenten auf **Fertig stellen**.

Sie können ein vorhandenes Proxyobjekt untersuchen, indem Sie den Befehl **Eigenschaften** für dieses Objekt ausführen. Das Dialogfeld **Eigenschaften** ermöglicht Ihnen, das von dem Proxyobjekt angegebene Benutzerkonto anzuzeigen. Aufgrund einer Einschränkung von AD LDS kann diese Einstellung jedoch nicht für ein vorhandenes Proxyobjekt geändert werden. Sie können ein Active Directory-Domänen-Benutzerkonto nur während der Erstellung des Proxyobjekts auswählen. Nach der Erstellung eines Proxyobjekts kann diese Einstellung nicht mehr geändert werden.

Wenn Sie ein Proxyobjekt erstellen, können Sie ein Benutzerkonto aus jeder beliebigen Domäne auswählen, die bei ActiveRoles Server registriert ist, vorausgesetzt, dass der Domäne von dem Computer vertraut wird, auf dem die AD LDS-Instanz ausgeführt wird.

Ein Proxyobjekt für einen Domänenbenutzer kann nicht in einer AD LDS-Verzeichnispartition erstellt werden, die bereits ein fremdes Prinzipalobjekt (FPO) oder ein Proxyobjekt für denselben Domänenbenutzer enthält.

Für ein bestimmtes Benutzerkonto in Active Directory können Sie eine Liste der Proxyobjekte anzeigen, die das Benutzerkonto in AD LDS angeben: Rufen Sie im Dialogfeld **Eigenschaften** für das Benutzerkonto die Registerkarte **Objekt** auf und klicken Sie dann auf **AD LDS-Proxyobjekt**.

Anpassen der Konfiguration von ActiveRoles Server

Nachfolgend sind die die AD LDS-Datenverwaltungsspezifischen und mit der Konfiguration von ActiveRoles Server verbundenen Aufgaben aufgeführt:

- **Bereitstellen von regelbasierten administrativen Ansichten** Sie können verwaltete Einheiten in ActiveRoles Server so konfigurieren, dass sie virtuelle Zusammenstellungen von Verzeichnisobjekten von AD LDS, Active Directory oder beiden für die Verteilung von administrativen Verantwortlichkeiten und für die Erzwingung von Geschäftsregeln und -richtlinien darstellen.
- **Implementieren einer rollenbasierten Delegation** Sie können ActiveRoles Server Zugriffsvorlagen anwenden, um die Kontrolle über AD LDS-Daten zu delegieren. Dies erfolgt auf gleiche Weise, wie Sie dies für die in Active Directory-Domänen gespeicherten Verzeichnisdaten tun.
- **Richtlinienbasierte Kontrolle und automatische Bereitstellung von Verzeichnisdaten** Sie können ActiveRoles Serverrichtlinienobjekte anwenden, um richtlinienbasierte Kontrollen einzurichten und die automatische Bereitstellung von AD LDS-Daten durchzuführen. Dies erfolgt auf gleiche Weise, wie Sie dies für die in Active Directory-Domänen gespeicherten Verzeichnisdaten tun.

In diesem Abschnitt wird jede dieser Aufgaben eingehend beschrieben.

Konfigurieren von verwaltete Einheiten für die Aufnahme von AD LDS-Objekten

Mit Hilfe der ActiveRoles Server-Konsole können Sie verwaltete Einheiten in ActiveRoles Server so konfigurieren, dass sie virtuelle Zusammenstellungen von Verzeichnisobjekten von AD LDS, Active Directory oder beiden für die Verteilung von administrativen Verantwortlichkeiten und für die Erzwingung von Geschäftsregeln darstellen. Bei Konfiguration verwalteter Einheiten, sodass diese Verzeichnisobjekte von jedem Speicherort (ganz gleich, ob es AD LDS oder Active Directory ist) aufnehmen können, bietet ActiveRoles Server die Möglichkeit, eine rollenbasierte Delegation und eine richtlinienbasierte administrative Kontrolle von Verzeichnisdaten ohne Berücksichtigung der Verzeichnisgrenzen zu implementieren, wo dies erforderlich ist.

Gehen Sie wie nachfolgend beschrieben vor, um eine vorhandene verwaltete Einheit so zu konfigurieren, dass sie AD LDS-Objekte wie etwa AD LDS-Benutzer, Gruppen oder Organisationseinheiten enthalten kann. Ausführlichere Anweisungen bezüglich der Erstellung und Verwaltung von verwalteten Einheiten finden Sie im Abschnitt „Regelbasierte administrative Ansichten“ weiter oben in diesem Dokument.

Gehen Sie folgendermaßen vor, um eine vorhandene verwaltete Einheit so zu konfigurieren, dass sie von einer Abfrage ausgegebene AD LDS-Objekte aufnimmt:

1. Klicken Sie mit der rechten Maustaste auf die verwaltete Einheit und klicken Sie dann auf **Eigenschaften**.
2. Klicken Sie auf der Registerkarte **Mitgliedschaftsregeln** auf **Hinzufügen**.
3. Klicken Sie im Dialogfeld **Mitgliedschaftsregeltyp** auf **Nach Abfrage einschließen** und klicken Sie dann auf **OK**.
4. Verwenden Sie das Dialogfeld **Mitgliedschaftsregel erstellen**, um die Abfrage einzurichten:
   a) Klicken Sie in der Liste **Suchen** auf **Benutzerdefinierte Suche**.
   b) Klicken Sie auf **Durchsuchen** neben dem Feld **In**.
   c) Erweitern Sie im Dialogfeld **Container suchen** den Container **AD LDS (ADAM)**, erweitern Sie dann die AD LDS-Verzeichnispartition, die die Objekte enthält, die die Abfrage ausgeben soll, und wählen Sie den Container, in dem sich diese Objekte befinden. Klicken Sie dann auf **OK**.
   d) Klicken Sie auf die Schaltfläche **Feld** und wählen Sie die Objekttypen, die die Abfrage ausgeben soll, sowie die Objekteigenschaft, die Sie abfragen möchten.
   e) Klicken Sie unter **Bedingung** auf die Bedingung für Ihre Abfrage und geben Sie dann unter **Wert** einen Eigenschaftswert ein, damit Ihre Abfrage die Objekte ausgibt, die die Objekteigenschaft haben, die mit dem von Ihnen angegebenen Bedingungswert-Paar übereinstimmen.
   f) Klicken Sie auf die Schaltfläche **Hinzufügen**, um diese Abfragebedingung zur Abfrage hinzuzufügen.
   g) Wiederholen Sie optional die Schritte d) bis f), um ihre Abfrage durch das Hinzufügen weiterer Bedingungen zu präzisieren. Wenn die Abfrage die Objekte ausgeben soll, die allen angegebenen Bedingungen entsprechen, klicken Sie auf **UND**. Wenn die Abfrage die Objekte ausgeben soll, die einer beliebigen der angegebenen Bedingungen entsprechen, klicken Sie auf **ODER**.
   h) Klicken Sie optional auf **Regelvorschau**, um eine Liste der Objekte anzuzeigen, die Ihre Abfrage ausgibt. Beachten Sie, dass die Abfrageergebnisse abhängig vom aktuellen Status der Daten im Verzeichnis variieren können. Die verwaltete Einheit wird die Abfrage immer dann, wenn Änderungen an den Verzeichnisdaten durchgeführt wurden, automatisch erneut anwenden, um zu gewährleisten, dass die Mitgliedschaftsliste der verwalteten Einheit aktuell und richtig ist.
   i) Klicken Sie auf die Schaltfläche **Regel hinzufügen**.
5. Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften** für die verwaltete Einheit zu schließen.

Sie können auch Mitgliedschaftsregeln von anderen Kategorien als „Nach Abfrage einschließen" konfigurieren, um AD LDS-Objekte aus einer verwalteten Einheit aufzunehmen bzw. auszuschließen. Wählen Sie hierzu die entsprechende Kategorie im Dialogfeld **Mitgliedschaftsregeltyp** aus. Weitere Schritte für die Konfiguration einer Mitgliedschaftsregel sind allesamt an die Verwendung des Dialogfelds **Mitgliedschaftsregel erstellen** für die Konfiguration einer bestimmten Abfrage oder an die Verwendung des Dialogfelds „Objekte auswählen" zum Auswählen eines bestimmten Objekts gebunden.

Anzeigen oder Festlegen von Berechtigungen für AD LDS-Objekte

Mit Hilfe der ActiveRoles Server-Konsole können Sie ActiveRoles Server Zugriffsvorlagen anwenden, um die Kontrolle über AD LDS-Daten zu delegieren. Dies erfolgt auf gleiche Weise, wie Sie dies für die in Active Directory-Domänen gespeicherten Verzeichnisdaten tun. Durch die Anwendung von Zugriffsvorlagen auf Benutzer oder Gruppen (Trustees) von AD LDS-Objekten und Containern können Sie die entsprechende Zugriffsebene auf die in AD LDS gespeicherten Verzeichnisdaten für die Trustees einrichten und sie somit zur Durchführung einer genau festgelegten Reihe von Aktivitäten befugen, die mit der AD LDS-Datenverwaltung in Verbindung stehen.

ActiveRoles Server bietet eine umfassende Palette an vorkonfigurierten Zugriffsvorlagen, um die Delegation von AD LDS-Datenverwaltungsaufgaben zu erleichtern. Eine Liste der AD LDS-spezifischen Zugriffsvorlagen finden Sie im Dokument *Sofort verwendbare Zugriffsvorlagen*, das Teil der ActiveRoles Server-Dokumentation ist. Diese Zugriffsvorlagen befinden sich im Container **Configuration/Access Templates/AD LDS (ADAM)** in der ActiveRoles Server-Konsole.

Gehen Sie wie nachfolgend beschrieben vor, um zu überprüfen, welche Zugriffsvorlagen auf ein bestimmtes AD LDS-Objekt wie etwa ein AD LDS-Benutzer, eine Gruppe, eine Organisationseinheit, ein Container oder die gesamte Verzeichnispartition angewandt wurden und um Zugriffsvorlagen hinzuzufügen oder zu entfernen, um die Ebene des Zugriffs zu ändern, den die Trustees auf dieses Objekt haben.

Ausführlichere Anweisungen bezüglich der Erstellung, Konfiguration und Anwendung von Zugriffsvorlagen finden Sie im Abschnitt „Rollenbasierte Administration" weiter oben in diesem Dokument.

Gehen Sie folgendermaßen vor, um die Liste der Zugriffsvorlagen für ein AD LDS-Objekt anzuzeigen oder zu ändern:

1. Wählen Sie in der Konsolenstruktur unter **AD LDS (ADAM)** den Container aus, der das Objekt enthält, für das Sie die Liste der Zugriffsvorlagen anzeigen oder ändern möchten.
2. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf das Objekt und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie auf der Registerkarte **Verwaltung** im Dialogfeld **Eigenschaften** auf **Sicherheit**.
4. Zeigen Sie im Dialogfeld **ActiveRoles Server-Sicherheit** die Liste der Zugriffsvorlagen an, die auf das AD LDS-Objekt angewandt wurden, oder ändern Sie die Liste wie folgt:
   - Um eine zusätzliche Zugriffsvorlage auf das Objekt anzuwenden, klicken Sie auf **Hinzufügen** und befolgen Sie die Anweisungen des Assistent für die Kontrolldelegierung.
   - Um von einer Zugriffsvorlage für das Objekt angegebene Berechtigungen zu entfernen, wählen Sie die Zugriffsvorlage in der Liste aus und klicken Sie dann auf **Entfernen**.
5. Klicken Sie auf **OK**, um das Dialogfeld **ActiveRoles Server-Sicherheit** zu schließen.
6. Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften** für das AD LDS-Objekt zu schließen.

Im Assistent für die Kontrolldelegierung können Sie die Benutzer oder Gruppen (Trustees) auswählen, die die Berechtigungen erhalten sollen, und wählen dann eine oder mehrere Zugriffsvorlagen aus dem Container **Access Templates/AD LDS (ADAM)** aus, um die Berechtigungen zu definieren. Als Folge haben die von Ihnen ausgewählten Trustees die Berechtigungen, die von den Zugriffsvorlagen für das AD LDS-Objekt definiert sind. Die Trustees können die Berechtigungen nur innerhalb von ActiveRoles Server ausführen, da ActiveRoles Server keine Berechtigungseinstellungen an AD LDS überträgt.

Im Dialogfeld **ActiveRoles Server-Sicherheit** kann eine Zugriffsvorlage nur entfernt werden, wenn sie auf das Objekt angewandt wird, das Sie ausgewählt haben (statt auf einen Container, in dem das Objekt gespeichert ist). Um die Zugriffsvorlagen anzuzeigen, die aus der aktuellen Auswahl entfernt werden können, deaktivieren Sie das Kontrollkästchen **Vererbung anzeigen**.

Anstatt eine Zugriffsvorlage im Dialogfeld **ActiveRoles Server-Sicherheit** zu entfernen, können Sie die Zugriffsvorlage auswählen und dann auf **Deaktivieren** klicken, um die Berechtigungen für die Objekte zurückzunehmen, die von der Zugriffsvorlage definiert sind. Auf diese Weise können Sie die Auswirkungen einer Zugriffsvorlage vermeiden, und zwar unabhängig davon, ob die Zugriffsvorlage auf das Objekt selbst oder auf einen Container, in dem sich das Objekt befindet, angewandt wird. Sie können diesen Vorgang rückgängig machen, indem Sie die Zugriffsvorlage auswählen und dann auf **Aktivieren** klicken.

Anzeigen oder Festlegen von Richtlinien für AD LDS-Objekte

Mit Hilfe der ActiveRoles Server-Konsole können Sie ActiveRoles Serverrichtlinienobjekte anwenden, um richtlinienbasierte Kontrollen einzurichten und die automatische Bereitstellung von AD LDS-Daten durchzuführen. Dies erfolgt auf gleiche Weise, wie Sie dies für die in Active Directory-Domänen gespeicherten Verzeichnisdaten tun. Durch die Bereitstellung der Möglichkeit, betriebliche Richtlinien streng durchzusetzen und einen nicht kontrollierten Zugriff auf sensible, in AD LDS gespeicherte Informationen zu unterbinden, gewährleistet die Hilfe von ActiveRoles Server die Sicherheit Ihrer unternehmenskritischen Daten. Richtlinienobjekte können so konfiguriert werden, dass sie eine Vielzahl von Richtlinien wie auf AD LDS angewandt festlegen. Hierzu zählen unter anderem die Überprüfung von Datenformaten, die regelbasierte, automatische Bereitstellung bestimmter Datenbereiche in AD LDS und skriptbasierte, benutzerdefinierte Vorgänge an AD LDS-Daten.

Gehen Sie wie nachfolgend beschrieben vor, um eine Liste der Richtlinienobjekte anzuzeigen oder zu ändern, die auf ein bestimmtes AD LDS-Objekt wie etwa einen AD LDS-Benutzer, eine Gruppe, eine Organisationseinheit, einen Container oder die gesamte Verzeichnispartition angewandt wurden. Ausführlichere Anweisungen bezüglich der Erstellung, Konfiguration und Anwendung von Richtlinienobjekten finden Sie im Abschnitt „Regelbasierte automatische Bereitstellung und Deprovisionierung" weiter oben in diesem Dokument.

Gehen Sie folgendermaßen vor, um die Liste der Richtlinienobjekte für ein AD LDS-Objekt anzuzeigen oder zu ändern:

1. Wählen Sie in der Konsolenstruktur unter **AD LDS (ADAM)** den Container aus, der das Objekt enthält, für das Sie die Liste der Richtlinienobjekte anzeigen oder ändern möchten.
2. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf das Objekt und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie auf der Registerkarte **Verwaltung** im Dialogfeld **Eigenschaften** auf **Richtlinie**.
4. Zeigen Sie im Dialogfeld **ActiveRoles Server-Richtlinie** die Liste der Richtlinienobjekte an, die Auswirkungen auf das AD LDS-Objekt haben, oder ändern Sie die Liste wie folgt:
   - Um ein weiteres Richtlinienobjekt auf das AD LDS-Objekt anzuwenden, klicken Sie auf **Hinzufügen**, wählen dann das anzuwendende Richtlinienobjekt aus und klicken Sie dann auf **OK**.
   - Um die Auswirkung eines Richtlinienobjekts auf das AD LDS-Objekt aufzuheben, wählen Sie das Richtlinienobjekt in der Liste aus und klicken Sie dann auf **Entfernen**. Aktivieren Sie alternativ dazu das Kontrollkästchen **Gesperrt** neben dem Namen des Richtlinienobjekts.
5. Klicken Sie auf **OK**, um das Dialogfeld **ActiveRoles Serverrichtlinie** zu schließen.
6. Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften** für das AD LDS-Objekt zu schließen.

Im Dialogfeld **ActiveRoles Serverrichtlinie** kann ein Richtlinienobjekt nur entfernt werden, wenn es auf das AD LDS-Objekt angewandt wird, das Sie ausgewählt haben (anstelle auf einen Container, in dem sich das AD LDS-Objekt befindet). Um die Richtlinienobjekte anzuzeigen, die aus der aktuellen Auswahl entfernt werden können, klicken Sie auf **Erweitert** und deaktivieren Sie dann das Kontrollkästchen **Vererbung anzeigen**.

Anstatt ein Richtlinienobjekt im Dialogfeld **ActiveRoles Serverrichtlinie** zu entfernen, können Sie das Kontrollkästchen **Gesperrt** in dem Listeneintrag für das Richtlinienobjekt aktivieren, um die Auswirkungen des Richtlinienobjekts auf das AD LDS-Objekt aufzuheben. Auf diese Weise können Sie die Auswirkungen eines Richtlinienobjekts vermeiden, und zwar unabhängig davon, ob das Richtlinienobjekt auf das AD LDS-Objekt selbst oder auf einen Container, in dem sich das Objekt befindet, angewandt wird. Wenn Sie ein Richtlinienobjekt für ein bestimmtes AD LDS-Objekt sperren, haben die von diesem Richtlinienobjekt definierten Richtlinieneinstellungen keine Auswirkungen mehr auf das AD LDS-Objekt. Sie können diese Vorgang durch Deaktivieren des Kontrollkästchens **Gesperrt** rückgängig machen.

15

Verwalten der Konfiguration von ActiveRoles Server

- Einleitung
- Herstellen einer Verbindung zum Verwaltungsdienst
- Hinzufügen und Entfernen verwalteter Domänen
- Konfigurieren der Replikation
- Verwenden der Datenbankspiegelung
- Erstellen und Verwenden virtueller Attribute
- Untersuchen von Client-Sitzungen
- Überwachen der Leistung
- Anpassen der Konsole

Einleitung

In diesem Kapitel werden die folgenden Verwaltungsaktivitäten untersucht:

- Herstellen einer Verbindung zum Verwaltungsdienst
- Registrieren von Domänen bei ActiveRoles Server
- Konfigurieren der Replikation des Verwaltungsdienstes
- Erstellen und Verwenden virtueller Attribute
- Untersuchen von Client-Sitzungen und Überwachen der Leistung
- Anpassen der ActiveRoles Server-Konsole

Um die Konfiguration des Verwaltungsdienstes zu administrieren, benötigen Sie geeignete Berechtigungen. Es genügt, Mitglied des Kontos AR Server Admin zu sein. Das Konto AR Server Admin wird beim Installieren des Verwaltungsdienstes angegeben. Es entspricht standardmäßig der Administratorengruppe auf dem Computer, auf dem der Verwaltungsdienst ausgeführt wird.

Die Autorisierung, die Konfiguration des Verwaltungsdienstes zu ändern, kann delegiert werden. Wenden Sie dazu die Zugriffsvorlage **Manage Configuration** auf den Container **Server Configuration** an.

Herstellen einer Verbindung zum Verwaltungsdienst

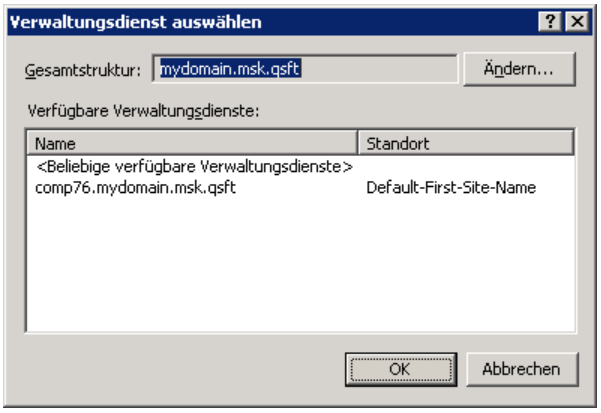
Um einen bestimmten Verwaltungsdienst mit Hilfe der ActiveRoles Server-Konsole zu konfigurieren, müssen Sie manuell den Verwaltungsdienst angeben, mit dem Sie eine Verbindung herstellen möchten. Andernfalls wählt die Konsole automatisch den Verwaltungsdienst aus.

Sie können das Dialogfeld **Verbindung zum Verwaltungsdienst herstellen** verwenden, um den entsprechenden Verwaltungsdienst manuell auszuwählen. Um dieses Dialogfeld anzuzeigen, klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf **ActiveRoles Server** und klicken Sie dann auf **Verbinden**. Das Dialogfeld entspricht der folgenden Abbildung.

Geben Sie im Fenster **Dienst** den Namen des Computers ein, auf dem der Verwaltungsdienst ausgeführt wird, zu dem eine Verbindung hergestellt werden soll, oder wählen Sie den Namen aus. Klicken Sie dann auf **Verbinden**. Das Feld **Dienst** bietet eine Liste der Namen, die für vorige Verbindungssitzungen angegeben wurden. Standardmäßig wird der zuletzt ausgewählte Name angezeigt.

Um einen nicht in der Liste aufgeführten Verwaltungsdienst auszuwählen, klicken Sie auf die Schaltfläche **Wählen** neben dem Feld **Dienst**:

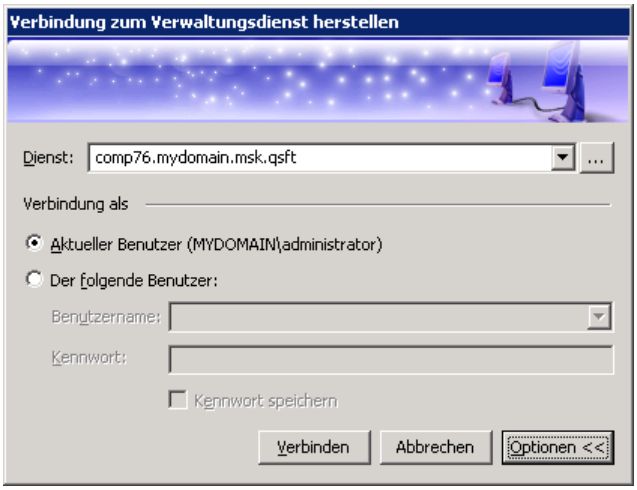
Hierdurch wird das Dialogfeld **Verwaltungsdienst auswählen** angezeigt, das in der folgenden Abbildung dargestellt ist.



Im Dialogfeld **Verwaltungsdienst auswählen** werden die Verwaltungsdienste aufgelistet, die in der angegebenen Gesamtstruktur verfügbar sind. Sie können eine andere Gesamtstruktur durch Anklicken von **Ändern** auswählen. Die Listenelemente sind nach Priorität sortiert. Dabei werden die Seite und die Auslastung des jeweiligen Dienstes beachtet (weniger stark ausgelastete Verwaltungsdienste werden in der Liste ganz oben angezeigt). Um einen bestimmten Dienst zum Dialogfeld **Verbindung zum Verwaltungsdienst herstellen** hinzuzufügen, klicken Sie auf den Dienst und klicken Sie dann auf **OK**.

Wenn Sie eine Verbindung zu einem bestimmten Dienst aufgebaut haben, versucht die Konsole, bei jedem weiteren Start automatisch eine Verbindung zu diesem Dienst aufzubauen. Wenn Sie die Option **<Beliebige verfügbare Verwaltungsdienste>** ausgewählt haben, versucht die Konsole, eine Verbindung zum nächsten, am wenigsten ausgelasteten Dienst in der angegebenen Gesamtstruktur aufzubauen, wobei die Dienste bevorzugt werden, die zur selben Replikationsgruppe wie der Dienst gehören, mit der die Konsole bei der letzten Sitzung verbunden war.

Standardmäßig baut die Konsole die Verbindung zum Verwaltungsdienst im Sicherheitskontext Ihres Anmeldekontos auf (d. h. das Benutzerkonto, mit dem Sie sich angemeldet haben). Das bedeutet, dass Sie die Konsole nur verwenden können, um die Aufgaben auszuführen, die an Ihr Benutzerkonto delegiert wurden. Sie haben die Option, eine Verbindung mit Hilfe eines anderen Kontos aufzubauen, um den Umfang der zulässigen Aufgaben zu erweitern. Klicken Sie auf **Optionen**, um das Dialogfeld **Verbindung zum Verwaltungsdienst herstellen** wie in der folgenden Abbildung gezeigt zu erweitern.



Klicken Sie auf **Der folgende Benutzer** und geben Sie dann Benutzeranmeldenamen und das Kennwort des Kontos an, das für die Verbindung verwendet werden soll. Durch Aktivieren des Kontrollkästchens **Kennwort speichern** verwendet die Konsole automatisch den angegebenen Benutzernamen und das Kennwort bei zukünftigen Verbindungssitzungen. Ansonsten fordert Sie die Konsole bei einem weiteren Start zur Eingabe eines Kennworts auf.

Schrittweise Anleitungen bezüglich des Verbindungsaufbaus zum Verwaltungsdienst finden Sie unter **Anleitungen/Verwalten von Konfiguration/Verbinden mit dem Verwaltungsdienst** in der ActiveRoles Server-Hilfe.

Hinzufügen und Entfernen verwalteter Domänen

Active Directory-Domänen, die bei ActiveRoles Server registriert sind, werden als *verwaltete Domänen* bezeichnet. Jeder Verwaltungsdienst pflegt eine Liste verwalteter Domänen und speichert diese Liste als Teil der Dienstkonfiguration in der Verwaltungsdatenbank.

In der ActiveRoles Server-Konsole wird der Assistent „Verwaltete Domäne hinzufügen" verwendet, um Domänen für die Verwaltung zu registrieren. Sie können auf folgende Weise auf den Assistenten zugreifen: Klicken Sie auf das Stammverzeichnis der Konsolenstruktur. Klicken Sie dann im Detailfenster im Bereich **Domänen** auf **Domäne hinzufügen**.

Der Assistent „Verwaltete Domäne hinzufügen" fordert Sie zur Eingabe der folgenden Informationen auf:

- Der Name der zu registrierenden Domäne.
- Die Rechtezuweisungen, mit denen ActiveRoles Server auf die Domäne zugreifen soll.

Sie können die standardmäßigen Rechtezuweisungen verwenden (das Dienstkonto des Verwaltungsdienstes) oder den Benutzernamen und das Kennwort eines anderen Kontos (des Außerkraftsetzungskontos) eingeben. In beiden Fällen muss das Konto über ausreichende Rechte in der verwalteten Domäne verfügen. Weitere Informationen finden Sie im Abschnitt „Zugriff auf verwaltete Domänen" im ActiveRoles Server – Erste Schritte.

Wenn Sie die Option für den Zugriff auf die verwaltete Domäne mit Hilfe der Dienstkontoinformationen auswählen, beachten Sie die folgenden Hinweise: Diese Option gilt für alle Verwaltungsdienste in Ihrer Umgebung. Jeder Verwaltungsdienst in Ihrer Umgebung verwendet für den Zugriff auf die Domäne sein eigenes Dienstkonto. Da verschiedene Dienstkonten über verschiedene Zugriffsebenen auf die Domäne verfügen können, kann ActiveRoles Server abhängig davon, welcher Verwaltungsdienst für die Verwaltung der Domäne verwendet wird, verschiedene Zugriffsrechte auf die Domäne haben. Aus diesem Grund kann das Verhalten von ActiveRoles Server bei einem Wechsel zu einem anderen Verwaltungsdienst variieren.

Nachdem Sie eine verwaltete Domäne hinzugefügt haben, ruft der Verwaltungsdienst die Domäneninformationen ab, z.B. das Active Directory-Schema und die Containerhierarchie. Dieser Prozess wird als *Laden von Domäneninformationen* bezeichnet.

Das Laden der Informationen in den Verwaltungsdienst kann einige Minuten dauern. Nach Abschluss dieses Prozesses steht die Domäne für die Verwaltung zur Verfügung. Wählen Sie in der Konsolenstruktur das Element **Active Directory** aus, und drücken Sie F5, um den Bereich „Details" zu aktualisieren und die neue Domäne anzuzeigen. Um die Verwaltung der Domäne zu starten, wählen Sie sie im Bereich „Details" aus und drücken Sie dann die Eingabetaste. Oder erweitern Sie das Domänenelement in der Konsolenstruktur.

Sie können eine Domäne aus der Liste der verwalteten Domänen entfernen. Danach können die Domäne und alle in ihr enthaltenen Verzeichnisobjekte nicht mehr mit ActiveRoles Server verwaltet werden. Um eine verwaltete Domäne zu entfernen, wählen Sie das Stammverzeichnis der Konsolenstruktur aus und klicken Sie dann auf **Zu verwalteten Domänen wechseln** im Bereich „Details" im Bereich **Domänen**. Hierdurch wird im Bereich „Details" eine Liste der verwalteten Domänen angezeigt. Klicken Sie in der Liste mit der rechten Maustaste auf die zu entfernende Domäne, und klicken Sie dann auf **Löschen**.

Schrittweise Anleitungen bezüglich des Hinzufügens und Entfernens von verwalteten Domänen finden Sie in den Themen **Hinzufügen einer verwalteten Domäne** und **Entfernen einer verwalteten Domäne** unter der Überschrift **Anleitungen/Konfiguration verwalten** in der ActiveRoles Server-Hilfe.

Konfigurieren der Replikation

ActiveRoles Server verwendet die Replikationsfunktionalität von Microsoft SQL Server, um Konfigurationsdaten aus Verwaltungsdienstdatenbanken zu kopieren und an andere zu verteilen und um die Daten in den Datenbanken im Interesse der Konsistenz miteinander zu synchronisieren.

Datenbankserver des Verwaltungsdienstes, die mit Hilfe der Replikationsfunktionalität von SQL Server synchronisiert werden, werden als *Replikationspartner* bezeichnet. Jeder Replikationspartner pflegt eine schreibbare Kopie der Konfigurationsdaten des Dienstes. Wenn Änderungen an einem Replikationspartner vorgenommen werden, werden diese auch an die anderen Replikationspartner weitergegeben.

Grundlegendes zum Replikationsmodell

In der ActiveRoles Server-Umgebung wird die Replikationsfunktionalität von SQL Server verwendet, um Änderungen an Konfigurationsdaten auf einem der Replikationspartner sofort an alle anderen Replikationspartner weiterzugeben. Nachdem Änderungen auf einem Replikationspartner festgeschrieben wurden, wird der Replikationsprozess wird sofort initiiert. ActiveRoles Server bietet keine Möglichkeit, dieses Verhalten zu ändern.

Da normalerweise nur wenige Änderungen vorliegen und da bei der Replikation nur geänderte Daten weitergegeben werden (Mergerreplikation), ist der Datenverkehr für die Replikation überschaubar. Daher müssen Sie die Replikation in ActiveRoles Server weder planen noch manuell erzwingen.

Bei der Mergereplikation ist normalerweise ein Lösungsmechanismus für Konflikte notwendig, die entstehen, wenn die gleichen Daten auf unterschiedlichen Replikationspartnern unterschiedlich geändert werden. Beim Replikationsmodell von ActiveRoles Server werden Konflikte aufgelöst, indem die letzte vorgenommene Änderung der betreffenden Daten ausgewählt wird.

Beim Replikationsmodell von ActiveRoles Server kann jeder Datenbankserver mit dem Verwaltungsdienst eine der folgenden Funktionen aufweisen:

- **Herausgeber** Der Publisher (Herausgeber) ist der Datenbankserver, der Daten für die Replikation anderen Replikationspartner verfügbar macht.

  Der Verwaltungsdienst, der den Publisher-Datenbankserver verwendet, wird als *Publisher-Verwaltungsdienst* bezeichnet.

- **Abonnent** Abonnenten sind Datenbankserver, die replizierte Daten empfangen. Abonnenten können Datenänderungen vom Publisher empfangen sowie Datenänderungen zurück an den Publisher weitergeben.

  Der Verwaltungsdienst, der einen Abonnenten-Datenbankserver verwendet, wird als *Abonnenten-Verwaltungsdienst* bezeichnet.

Replikationsgruppe

Der Publisher und seine Abonnenten bilden zusammen eine Replikationsgruppe. Jede Replikationsgruppe muss genau einen Publisher enthalten und kann beliebig viele Abonnenten enthalten. Die Mitglieder einer Replikationsgruppe werden als *Replikationspartner* bezeichnet.

Jedes Mitglied einer Replikationsgruppe (jeder Replikationspartner) pflegt eine eigene, schreibbare Kopie der Konfigurationsdaten des Verwaltungsdienstes. Die Replikation kopiert und verteilt Daten zwischen Mitgliedsdatenbanken und synchronisiert im Interesse der Konsistenz Daten zwischen den Datenbanken. Wenn Änderungen auf dem Publisher vorgenommen werden, repliziert der Publisher sie an jeden Abonnenten. Wenn Datenänderungen auf einem Abonnenten vorgenommen werden, leitet der Abonnent sie an den Publisher weiter, der sie dann an jeden Abonnenten repliziert.

Dieser Replikationsprozess stellt sicher, dass alle Verwaltungsdienste, die die Datenbankserver in der Replikationsgruppe verwenden, die gleiche Konfiguration aufweisen.

Wenn ein Datenbankserver mit dem Verwaltungsdienst eingerichtet wird, wird er zunächst als *allein stehende Datenbank* konfiguriert. Er hat also keine Replikationspartner und gehört keiner Replikationsgruppe an. Der Verwaltungsdienst, der einen allein stehenden Datenbankserver verwendet, wird als *allein stehender Verwaltungsdienst* bezeichnet.

Sie können einen allein stehenden Datenbankserver einer beliebigen vorhandenen Replikationsgruppe hinzufügen. Dann wird der Datenbankserver ein Abonnent. Jeder Datenbankserver mit dem Verwaltungsdienst darf nur einer Replikationsgruppe angehören. Nachdem er aus einer Replikationsgruppe entfernt wurde, kann er einer anderen hinzugefügt werden.

Um eine neue Replikationsgruppe zu erstellen, muss ein allein stehender Datenbankserver als Publisher ausgewählt werden. Dann enthält die neue Replikationsgruppe ein einziges Mitglied, den Publisher. Später können Sie der Gruppe Abonnenten hinzufügen.

Wenn in ActiveRoles Server Replikationsfehler auftreten, ist dies auf der ActiveRoles Server-Konsole sichtbar, da in der Konsolenstruktur ein anderes Symbol für die Container **Server Configuration** und **Configuration Databases** verwendet wird: Neben jedem dieser Container wird eine Beschriftung mit einem Ausrufezeichen angezeigt. So kann der Administrator einen Replikationsfehler erkennen, ohne einzelne Replikationspartner zu untersuchen.

Konfigurieren von SQL Server

Um sicherzustellen, dass SQL Server für die Verwaltungsdienstreplikation ordnungsgemäß konfiguriert ist, prüfen Sie, ob der SQL Server-Agent-Dienst gestartet wurde und ordnungsgemäß konfiguriert ist.

Der SQL Server-Agentendienst muss auf dem Datenbankserver mit SQL Server ausgeführt werden, der als Publisher dient. Sie sollten den Starttyp für diesen Dienst auf **Automatisch** festlegen.

Der SQL Server-Agentendienst sollte so konfiguriert sein, dass er sich mit einem Domänenbenutzerkonto anmeldet. Das Anmeldekonto muss ein Systemadministratorkonto (Mitglied der festen Serverrolle **Systemadministrator**) auf dem Publisher mit SQL Server sein.

Wenn eine Replikationsgruppe Abonnenten enthält, die die Windows-Authentifizierung (integrierte Authentifizierung) verwenden, muss das Anmeldekonto des SQL Server-Agentendienstes außerdem der Rolle **Systemadministrator** auf jedem dieser Abonnenten mit SQL Server angehören.

Weitere Informationen über die Berechtigungen für SQL Server, die für einen ordnungsgemäßen Betrieb der Verwaltungsdienstreplikation erforderlich sind, finden Sie im Abschnitt „SQL Server-spezifische Berechtigungen" im Dokument *ActiveRoles Server-Replikation*: *Empfohlene Vorgehensweisen und Fehlerbehebung*.

Gehen Sie folgendermaßen vor, um den SQL Server-Agentendienst zu konfigurieren:

1. Erstellen Sie ein Domänenbenutzerkonto.
2. Fügen Sie auf dem Publisher-Computer mit SQL Server das Konto zur lokalen Administratorengruppe hinzu.
3. Fügen Sie auf dem Publisher-Computer mit SQL Server das Konto zur Rolle **Systemadministrator** hinzu.
4. Wenn die Replikationsgruppe Abonnenten mit der Windows-Authentifizierung enthält, fügen Sie das Konto auf jedem dieser Abonnenten mit SQL Server zur Rolle **Systemadministrator** hinzu.
5. Konfigurieren Sie auf dem Publisher-Computer mit SQL Server den SQL Server-Agentendienst so, dass er sich mit dem dafür vorbereiteten Konto anmeldet, und starten Sie den Dienst dann neu.

Informationen bezüglich des Hinzufügens eines Benutzerkontos zur Rolle **Systemadministrator** auf SQL Server finden Sie im Hilfethema „Adding a Member to a Predefined Role" in der Online-Dokumentation von SQL Server.

Erstellen einer Replikationsgruppe

Um eine Replikationsgruppe zu erstellen, wählen Sie einen allein stehenden Datenbankserver mit dem Verwaltungsdienst als Publisher aus. Sie können dazu die ActiveRoles Server-Konsole wie folgt verwenden:

1. Stellen Sie eine Verbindung zu einem autonomen Verwaltungsdienst her.
2. Stufen Sie den Datenbankserver mit dem Verwaltungsdienst zum Publisher herauf.

Um eine Verbindung zum Verwaltungsdienst herzustellen, gehen Sie gemäß den weiter oben in diesem Kapitel aufgeführten Anweisungen vor (siehe „Verbinden mit dem Verwaltungsdienst").

Nachdem Sie eine Verbindung mit dem Verwaltungsdienst hergestellt haben, führen Sie die folgenden Schritte aus, um die Verwaltungsserver-Datenbank zum Publisher heraufzustufen:

1. Wechseln Sie in der Konsolenstruktur zum Container **Configuration/Server Configuration/Configuration Databases**.
2. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf die Datenbank und klicken Sie dann auf **Heraufstufen**.

Der Befehl **Heraufstufen** wird nur angezeigt, wenn der Verwaltungsdienst einen allein stehenden Datenbankserver verwendet, d.h. einen Datenbankserver, der keiner Replikationsgruppe angehört.

Nachdem Sie auf **Heraufstufen** geklickt haben, dauert das Abschließen des Vorgangs mehrere Minuten. Nach Abschluss des Vorgangs enthält die neue Replikationsgruppe ein einziges Mitglied, den Publisher. Nach der Erstellung der Replikationsgruppe können Sie ihren Replikationspartner hinzufügen, die Abonnenten.

Hinzufügen von Mitgliedern zu einer Replikationsgruppe

Um einer Replikationsgruppe ein Mitglied hinzuzufügen, wählen Sie einen allein stehenden Datenbankserver als Abonnenten des Publisher der Gruppe aus. Sie können dazu die ActiveRoles Server-Konsole wie folgt verwenden:

1. Stellen Sie eine Verbindung zum Publisher-Verwaltungsdienst her.
2. Starten Sie den Assistenten „Neuer Replikationspartner" und schließen Sie ihn ab.

Zeigen Sie nach dem Herstellen der Verbindung zum Publisher-Verwaltungsdienst den Inhalt des Containers **Configuration Databases** an. Im Bereich „Details" werden die Namen des Publisher und seiner Abonnenten aufgelistet. Klicken Sie mit der rechten Maustaste auf den Publisher, und klicken Sie dann auf **Replikationspartner hinzufügen**. Folgen Sie dann den Anweisungen des Assistenten „Neuer Replikationspartner".

Klicken Sie auf der Seite **Datenbankauswahl** auf **Durchsuchen**, um den Verwaltungsdienst auszuwählen, der den als Abonnenten vorgesehenen Datenbankserver verwendet. Durch Anklicken von **Durchsuchen** wird ein Dialogfeld angezeigt, das identisch mit dem im Abschnitt „Verbinden mit dem Verwaltungsdienst" weiter oben in diesem Kapitel beschriebenen Dialogfeld ist. Geben Sie den Namen des Computers mit dem Verwaltungsdienst ein, oder wählen Sie ihn in der Liste aus.

Der Assistent wählt automatisch den Datenbankserver aus, der Host der Konfigurationsdatenbank des angegebenen Verwaltungsdienstes ist. Die nächste Seite des Assistenten zeigt den Datenbanknamen und die Datenbankspeicherposition an, die vom angegebenen Dienst abgefragt wurden. Außerdem werden Sie aufgefordert, eine der folgenden Optionen auszuwählen, die festlegen, wie der SQL Server-Agent, der auf dem Publisher SQL Server ausgeführt wird, die Verbindung zum Subscriber SQL Server aufbaut:

- **SQL Server Agent-Dienstkonto verkörpern** Verwenden Sie diese Option, wenn der SQL Server-Agent auf dem Publisher SQL Server so konfiguriert ist, dass er sich als ein Windows-Benutzerkonto anmeldet, das über ausreichende Rechte auf dem Subscriber SQL Server verfügt. Dieses Konto muss vor allem zur Rolle **Systemadministrator** auf dem Subscriber SQL Server gehören.
- **SQL Server-Authentifizierung mit folgendem Benutzernamen und Kennwort verwenden** Verwenden Sie diese Option, wenn das Anmeldekonto für den SQL Server-Agentendienst nicht so konfiguriert werden kann, dass es über ausreichende Rechte auf dem Subscriber SQL Server verfügt (zum Beispiel wenn der Publisher SQL Server und der Subscriber SQL Server in verschiedenen Gesamtstrukturen implementiert sind). Sie werden aufgefordert, das SQL Server-Login und Kennwort anzugeben, das der SQL Server Agent auf dem Publisher SQL Server für den Zugriff auf den Subscriber SQL Server verwenden wird. Das Login muss zur Rolle **Systemadministrator** auf dem Subscriber SQL Server gehören.

Auf der Abschlussseite des Assistenten können Sie Zusammenfassungsinformationen zu dem Datenbankserver überprüfen, den Sie als Abonnenten einrichten möchten. Nachdem Sie auf **Fertig stellen** klicken, wird der Datenbankserver der Replikationsgruppe hinzugefügt. Der Replikationsprozess aktualisiert die Datenbank des neuen Abonnenten mit den Daten, die vom Publisher abgerufen wurden.

Der Publisher kopiert neue Daten in die Datenbank und überschreibt dabei die vorhandenen Daten. Wenn die Datenbank wichtige Informationen (z.B. benutzerdefinierte Zugriffsvorlagen oder Richtlinienobjekte) enthält, sollten Sie diese Objekte exportieren, bevor Sie den Datenbankserver als Abonnenten festlegen, und sie nach Abschluss des Vorgangs wieder importieren.

Ein Datenbankserver kann nur dann einer Replikationsgruppe hinzugefügt werden, wenn er noch keiner anderen Replikationsgruppe angehört. Gehört er schon einer anderen an, wird ein Fehler angezeigt. Um den Datenbankserver einer anderen Replikationsgruppe hinzuzufügen, müssen Sie ihn zuerst aus der aktuellen Replikationsgruppe entfernen und ihn dann der anderen hinzufügen.

Entfernen von Mitgliedern aus einer Replikationsgruppe

Sie können mit Hilfe der ActiveRoles Server-Konsole Abonnenten wie folgt aus einer Replikationsgruppe entfernen:

1. Stellen Sie eine Verbindung zum Publisher-Verwaltungsdienst her.
2. Wählen Sie im Container **Configuration Databases** einen Abonnenten aus, klicken Sie mit der rechten Maustaste auf den Abonnenten, und klicken Sie dann auf **Löschen**.

Mit dieser Methode können Sie nur Abonnenten entfernen. Der Publisher kann nicht aus seiner Replikationsgruppe entfernt werden, während sie Abonnenten enthält.

Um den Publisher zu entfernen, müssen Sie erst alle Abonnenten entfernen und dann den Publisher herabstufen. Diese Aktion löscht die gesamte Replikationsgruppe.

Nachdem Sie alle Abonnenten entfernt haben, können Sie den Publisher wie folgt herabstufen: Klicken Sie im Container **Configuration Databases** mit der rechten Maustaste auf den Publisher und klicken Sie dann auf **Herabstufen**.

Schrittweise Anleitungen bezüglich der Konfiguration der Replikation in ActiveRoles Server finden Sie unter **Anleitungen/Verwalten von Konfiguration/Konfigurieren der Replikation** in der ActiveRoles Server-Hilfe.

Überwachung der Replikation

Mit ActiveRoles Server können Sie den Status von Replikationspartnern überwachen. Mit Hilfe der Überwachung können Sie bestimmen, ob die Replikation von ActiveRoles Server effizient und richtig arbeitet. Sie können den Status eines Replikationspartners wie folgt über die ActiveRoles Server-Konsole anzeigen:

1. Stellen Sie eine Verbindung mit einem beliebigen Verwaltungsdienst in der Replikationsgruppe her.
2. Öffnen Sie das Dialogfeld **Eigenschaften** für den Replikationspartner, und öffnen Sie die Registerkarte **Replikationsstatus**.

Um eine Verbindung zum Verwaltungsdienst herzustellen, gehen Sie gemäß den weiter oben in diesem Kapitel aufgeführten Anweisungen vor (siehe „Verbinden mit dem Verwaltungsdienst").

Nachdem Sie eine Verbindung mit dem Verwaltungsdienst hergestellt haben, öffnen Sie in den folgenden Schritten das Dialogfeld **Eigenschaften** für einen Replikationspartner:

1. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration | Server Configuration** und wählen Sie dann **Configuration Databases**.
2. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf den Replikationspartner, und klicken Sie dann auf **Eigenschaften**.

Im Dialogfeld **Eigenschaften** werden auf der Registerkarte **Replikationsstatus** Information zur letzten Replikationsaktion des Partners bereitgestellt, und es wird angezeigt, ob die Aktion erfolgreich abgeschlossen wurde, einen Fehler generiert hat oder noch ausgeführt wird.

Wenn in ActiveRoles Server Replikationsfehler auftreten, ist dies auf der ActiveRoles Server-Konsole sichtbar, da in der Konsolenstruktur ein anderes Symbol für die Container **Server Configuration** und **Configuration Databases** verwendet wird. So können Sie einen Replikationsfehler erkennen, ohne einzelne Datenbanken zu untersuchen.

Weitere Informationen über die Überwachung der Funktionsfähigkeit der ActiveRoles Server-Replikation finden Sie im Dokument *Quest ActiveRoles Server-Replikation: Empfohlene Vorgehensweisen und Fehlerbehebung*.

Verwenden der Datenbankspiegelung

Mit der Version 6.5 kann ActiveRoles Server die Microsoft SQL Server-Datenbankspiegelungstechnik nutzen, um die Verfügbarkeit des Verwaltungsdienstes zu verbessern. Die Datenbankspiegelung bietet einen Standby-Datenbankserver, der Failover unterstützt. Wenn der aktuelle Datenbankserver ausfällt, kann der Verwaltungsdienst schnell durch einen automatischen Verbindungsaufbau zum Standby-Server wiederhergestellt werden (dieser Vorgang wird als „Failover" bezeichnet).

Die Datenbankspiegelung erhöht die Datenbankverfügbarkeit durch Unterstützung eines schnellen Failovers. Diese Technologie kann verwendet werden, um zwei Kopien einer einzelnen ActiveRoles Server-Datenbank auf verschiedenen Serverinstanzen des SQL Server-Datenbankmoduls zu pflegen. Eine Serverinstanz bedient die Datenbank für den Verwaltungsdienst; diese Instanz wird als *Hauptserver* bezeichnet. Die andere Instanz fungiert als ein Standby-Server; diese Instanz wird als *Spiegelserver* bezeichnet.

Funktionswechsel

Im Zusammenhang mit der Datenbankspiegelung fungiert der Spiegelserver als der Failover-Partner für den Hauptserver. Bei einem Notfall übernimmt der Spiegelserver die Funktion des Hauptservers und stellt die gespiegelte Kopie der Datenbank als neue Hauptdatenbank online. Der ehemalige Hauptserver übernimmt dann, sofern er wieder verfügbar ist, die Funktion des Spiegelservers. Dieser als *Funktionswechsel* bekannte Vorgang kann in folgender Form erfolgen:

- **Automatischer Failover** Wenn der Hauptserver ausfällt, wird bei Auswahl dieser Option die gespiegelte Kopie der Datenbank schnell als neue Hauptdatenbank online verfügbar gemacht.
- **Manueller Failover** Ermöglicht dem Datenbankbesitzer, die Funktionen der Failover-Partner bei Bedarf umzukehren.
- **Forcierter Dienst** Wenn der Hauptserver ausfällt, ermöglicht diese Option dem Datenbankbesitzer, den Zugriff auf die Datenbank wiederherzustellen, indem er den Spiegelserver zur Übernahme der Funktion des Hauptservers zwingt.

Bei jedem Funktionswechsel kann der Verwaltungsdienst, sobald der neue Hauptdatenbank online ist, wiederhergestellt werden, indem er automatisch wieder die Verbindung zur Datenbank aufbaut.

Weitere Informationen über die Datenbankspiegelungstechnologie und Anweisungen bezüglich der Einrichtung und Verwaltung der Datenbankspiegelung auf dem SQL Server finden Sie unter dem Thema „Datenbankspiegelung" in der SQL Server-Produktdokumentation unter http://msdn.microsoft.com/en-us/library/bb934127.aspx.

In der Version 6.5 wird die ActiveRoles Server-Replikationsfunktion nicht für die Datenbanken unterstützt, für die eine Spiegelung eingerichtet ist. Wenn Sie versuchen, den Vorgang „An Herausgeber veröffentlichen" oder „Abonnent hinzufügen" für eine solche Datenbank durchzuführen, wird ein Fehler ausgegeben.

Einrichtung der Datenbankspiegelung in ActiveRoles Server

Es wird davon ausgegangen, dass die Spiegelung der Datenbank von ActiveRoles Server bereits SQL Server-seitig in Übereinstimmung mit den Empfehlungen und Anweisungen in der Dokumentation von Microsoft eingerichtet wurde, sodass die folgenden Bedingungen erfüllt sind:

- Der Verwaltungsdienst ist mit der Konfigurationsdatenbank auf dem Hauptdatenbankserver verbunden.
- Es ist keine Replikation für die Konfigurationsdatenbank konfiguriert (der Datenbankserver fungiert als ein autonomer Server, wie auf die ActiveRoles Server-Replikation angewandt).
- Der Verwaltungsdienst ist mit der Verwaltungsverlaufsdatenbank auf dem Hauptdatenbankserver verbunden (Standardmäßig ist die Verwaltungsverlaufsdatenbank mit der Konfigurationsdatenbank identisch).
- Es ist keine Replikation für die Verwaltungsverlaufsdatenbank konfiguriert (der Datenbankserver fungiert als ein autonomer Server, wie auf die ActiveRoles Server-Replikation angewandt).

Unter diesen Bedingungen kann der Verwaltungsdienst angewiesen werden, bei einem Wechsel der Datenbankserverfunktion automatisch eine Verbindung zur neuen Hauptdatenbank herzustellen. Fügen Sie auf dem Computer, auf dem der Verwaltungsdienst ausgeführt wird, einen Zeichenkettenwert zu jedem dieser beiden Registrierungsschlüssel hinzu und starten Sie dann den Verwaltungsdienst neu:

- **Schlüssel:** HKLM\SOFTWARE\Aelita\Enterprise Directory Manager\DatabaseConnectionString\
  Wertname: Failover Partner
  Wertdaten: *<Gibt die SQL Server-Instanz an, die aktuell die Spiegelserverfunktion für die Konfigurationsdatenbank inne hat.>*
- **Schlüssel:** HKLM\SOFTWARE\Aelita\Enterprise Directory Manager\CHDatabaseConnectionString\
  Wertname: Failover Partner
  Wertdaten: *<Gibt die SQL Server-Instanz an, die aktuell die Spiegelserverfunktion für die Verwaltungsverlaufsdatenbank inne hat.>*

Wenn die Standardinstanz verwendet wird, sind die Wertdaten der NetBIOS-Name des Computers, der SQL Server ausführt. Andernfalls sind die Wertdaten der NetBIOS-Name des Computers, gefolgt von einem umgekehrten Schrägstrich, gefolgt vom Namen der Instanz (wie etwa *Computername**Instanzname*).

Standardmäßig wird dieselbe Datenbank für die Konfigurations- und Verwaltungsverlaufsdaten verwendet; daher sind die Wertdaten in den Schlüsseln „DatabaseConnectionString" und „CHDatabaseConnectionString" identisch.

In der ActiveRoles Server-Konsole können Sie den Spiegelungsstatus der Konfigurations- oder Verwaltungsverlaufsdatenbank anzeigen, die von einer bestimmten Instanz des Verwaltungsdienstes verwendet wird:

1. Wählen Sie in der Konsolenstruktur **Configuration | Server configuration | Administration Services**.
2. Doppelklicken Sie im Bereich „Details" auf den Namen des Verwaltungsdienstes, dessen Datenbank Sie untersuchen möchten.

3. Klicken Sie im Dialogfeld **Eigenschaften** auf die Registerkarte **Konfigurationsdatenbank** oder **Verwaltungsverlaufsdatenbank** und lesen Sie die Informationen im Bereich **Datenbankspiegelung**:
   - **Funktion** Aktuelle Funktion der Datenbank in der Datenbankspiegelungssitzung (Hauptdatenbank oder gespiegelte Datenbank).
   - **Partner** Der Instanzname und Computername für den anderen Partner in der Datenbankspiegelungssitzung.
   - **Status** Aktueller Status der gespiegelten Datenbank und der Datenbankspiegelungs-sitzung. Weitere Informationen über dieses Feld finden Sie unter dem Thema „Spiegelungszustände" unter http://msdn.microsoft.com/en-us/library/ms189284.aspx.

   Wenn keine Informationen im Bereich **Datenbankspiegelung** angezeigt werden, dann ist die Datenbankspiegelung nicht konfiguriert.

Sie können den Spiegelungsstatus einer Konfigurationsdatenbank oder einer Verwaltungs-verlaufsdatenbank auch auf der Registerkarte **Allgemein** im Dialogfeld **Eigenschaften** für das Objekt anzeigen, das die Datenbank im Container **Configuration/Server Configuration/Configuration Databases** bzw. **Configuration/Server Configuration/Management History Databases** angibt.

Erstellen und Verwenden virtueller Attribute

Mit ActiveRoles Server können Sie benutzerdefinierte (virtuelle) Attribute für jeden beliebigen vorhandenen Objekttyp definieren. So können Sie zusätzliche Objekteigenschaften angeben, ohne das Active Directory-Schema zu erweitern. Beispielsweise können benutzerdefinierte Attribute verwendet werden, um bestimmte Benutzerdaten zu speichern.

Sie können ein virtuelles Attribut konfigurieren, um den Attributwert in der Datenbank von ActiveRoles Server zu speichern. Ansonsten müssen Sie für die Verwendung des virtuellen Attributs eine Skriptrichtlinie implementieren, die den Attributwert verarbeitet.

Wenn Sie Attributwerte in der Datenbank von ActiveRoles Server speichern, kann die Datenbank deutlich größer werden.

So erstellen Sie ein virtuelles Attribut:

1. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration | Server Configuration**.
2. Klicken Sie unter **Server Configuration** mit der rechten Maustaste auf **Virtual Attributes** und wählen Sie **Neu | Virtuelles Attribut** aus.
3. Folgen Sie den Anweisungen des Assistenten zum Hinzufügen eines virtuellen Attributs.
4. Geben Sie in die Felder **Allgemeiner Name** und **LDAP-Anzeigename** einen allgemeinen Namen und einen LDAP-Anzeigenamen für das neue Attribut ein.

   *Im Feld **Eindeutige X.500 Objekt-ID** können Sie optional den Standardwert der Eigenschaft „attributeID" (OID) für das neue Attribut ändern. Der Standardwert wird automatisch generiert. Wenn Sie einen eigenen Wert generieren möchten, können Sie das Tool Oidgen (oidgen.exe) im Windows Server Resource Kit verwenden.*

   *Im Feld **Schemakennungs-GUID** können Sie optional den Standardwert der Eigenschaft „schemaIDGUID" ändern. Der Standardwert wird automatisch generiert. Wenn das neue Attribut einen festen Wert für die Eigenschaft „schemaIDGUID" haben soll, ersetzen Sie den Standardwert durch den gewünschten Wert. Beispielsweise können Sie die GUID mit dem Tool Uuidgen im Microsoft Platform SDK generieren.*

5. Optional können Sie in das Feld **Beschreibung** eine Beschreibung für das neue virtuelle Attribut eingeben. Klicken Sie auf **Weiter**.
6. Klicken Sie in der Liste **Syntax** auf die gewünschte Syntax für das neue virtuelle Attribut. Wenn das neue Attribut mehrwertig sein soll, aktivieren Sie das Kontrollkästchen **Mehrere Werte**. Klicken Sie auf **Weiter**.
7. Aktivieren Sie die Kontrollkästchen neben den Objektklassen, denen Sie das virtuelle Attribut zuordnen möchten. Klicken Sie auf **Weiter**.

   *Wenn Sie das neue Attribut Objektklassen zuordnen möchten, die nicht standardmäßig aufgelistet sind, aktivieren Sie das Kontrollkästchen **Alle mögliche Klassen anzeigen**.*
8. Wenn Sie die Werte des Attributs in der Datenbank von ActiveRoles Server speichern möchten, aktivieren Sie das Kontrollkästchen auf der Seite **Attributspeicherung**.

   Wenn Sie die Attributwerte nicht in der Datenbank speichern möchten, ist eine Skriptrichtlinie erforderlich, die beim Abrufen des Attributs den Attributwert bereitstellt und beim Aktualisieren des Attributs den Attributwert speichert.

   Sie sollten diese Option jedoch mit Bedacht verwenden. Wenn Sie Attributwerte in der Konfigurationsdatenbank von ActiveRoles Server speichern, kann die Datenbank deutlich größer werden.

   Diese Option kann nach der Erstellung des Attributs mit Hilfe der Verwaltungsfunktionen für Eigenschaften des virtuellen Attributs geändert werden.
9. Klicken Sie auf **Weiter**, und klicken Sie dann auf **Fertig stellen**, um den Assistenten abzuschließen.

Stellen Sie nach dem Hinzufügen des neuen virtuellen Attributs erneut eine Verbindung mit dem Verwaltungsdienst her. Das neue virtuelle Attribut wird im Container **Virtual Attributes** unter **Configuration/Server Configuration** angezeigt.

Weitere Informationen zu virtuellen Attributen finden Sie in der ActiveRoles Server SDK-Dokumentation.

Schrittweise Anleitungen bezüglich der Verwendung des Assistenten zum Hinzufügen virtueller Attribute finden Sie unter **Anleitungen/Verwalten der Konfiguration/Virtuelles Attribut erstellen** in der ActiveRoles Server-Hilfe.

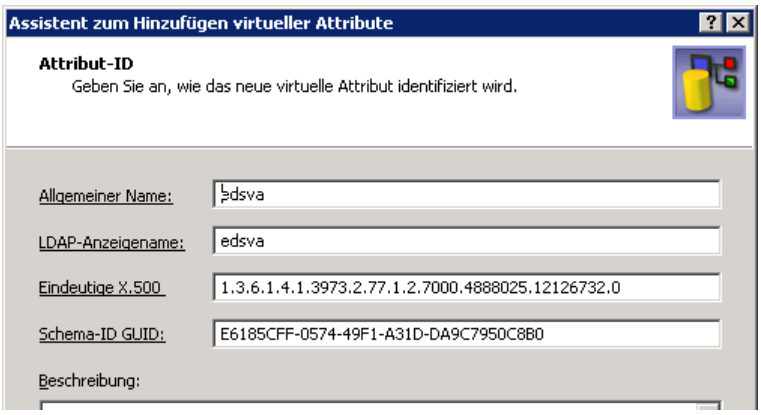
Szenario: Implementieren eines Attributs für den Geburtstag

In diesem Szenario wird veranschaulicht, wie Sie ein virtuelles Attribut erstellen und verwenden, um Informationen zu den Geburtstagen der Benutzer zu speichern.

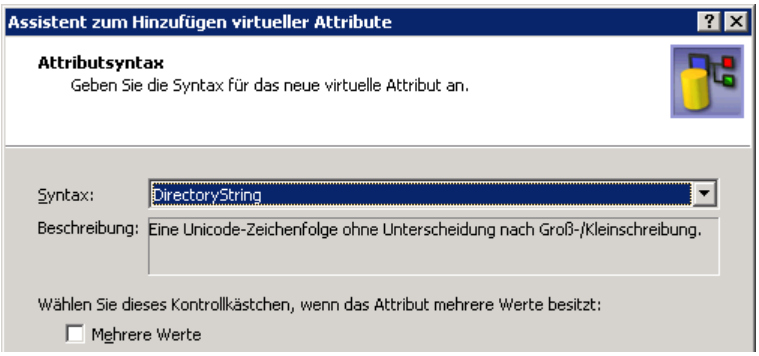
So erstellen Sie das Attribut für den Geburtstag:

1. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration | Server Configuration**.
2. Klicken Sie unter **Server Configuration** mit der rechten Maustaste auf **Virtual Attributes** und wählen Sie **Neu | Virtuelles Attribut** aus.
3. Klicken Sie auf **Weiter**.

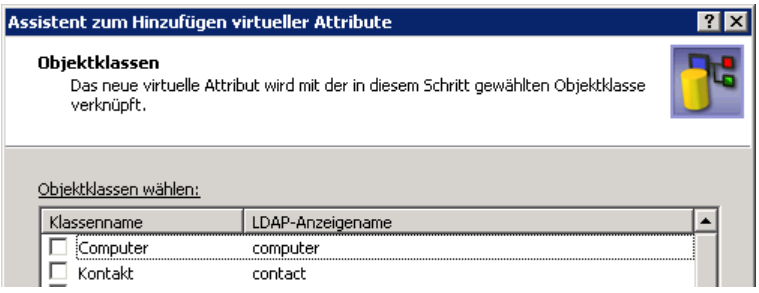
4. Geben Sie in die Felder **Allgemeiner Name** und **LDAP-Anzeigename** jeweils den Wert **Geburtstag** ein, wie in der folgenden Abbildung gezeigt.



5. Klicken Sie auf **Weiter**.
   *Die Seite **Attributsyntax** sollte nun der folgenden Abbildung entsprechen.*


Assistent zum Hinzufügen virtueller Attribute
Attributsyntax
Geben Sie die Syntax für das neue virtuelle Attribut an.
Syntax:
DirectoryString
Beschreibung:
Eine Unicode-Zeichenfolge ohne Unterscheidung nach Groß-/Kleinschreibung.
Wählen Sie dieses Kontrollkästchen, wenn das Attribut mehrere Werte besitzt:
Mehrere Werte

6. Klicken Sie auf **Weiter**.
7. Aktivieren Sie auf der Seite **Objektklassen** das Kontrollkästchen neben **Benutzer**, wie in der folgenden Abbildung gezeigt.



8. Klicken Sie auf **Weiter**.
9. Aktivieren Sie im Fenster für die Attributspeicherung das Kontrollkästchen **Werte dieses virtuellen Attributs in der ActiveRoles Verwaltungsdatenbank speichern**.
10. Klicken Sie auf **Weiter**, und klicken Sie dann auf **Fertig stellen**, um den Assistenten abzuschließen.

Stellen Sie zum Aktivieren des neuen Attributs wie folgt erneut eine Verbindung mit dem Verwaltungsdienst her: Klicken Sie mit der rechten Maustaste auf den Stamm der Konsolenstruktur und klicken Sie dann auf **Erneut verbinden**.

In der ActiveRoles Server-Konsole können Sie das Attribut **Geburtsdatum** für ein Benutzerkonto wie folgt verwalten:

1. Klicken Sie mit der rechten Maustaste auf das Benutzerkonto und wählen Sie **Alle Aufgaben | Erweiterte Eigenschaften** aus.
2. Aktivieren Sie im Dialogfeld **Erweiterte Eigenschaften** die Kontrollkästchen **Alle möglichen Attribute anzeigen** und **Attribute mit leeren Werten einschließen**.
3. Klicken Sie in der Liste der Eigenschaften auf **Geburtstag** und klicken Sie dann auf **Bearbeiten**.
4. Geben Sie in das Feld **Wert** einen Geburtstag ein.
5. Klicken Sie auf **OK**.

Sie können das Attribut **Geburtsdatum** auf über das ActiveRoles Server Web-Interface verwalten.

Fügen Sie zunächst das Feld **Geburtsdatum** dem Formular hinzu, auf dem Benutzereigenschaften angezeigt werden, und ordnen Sie dieses Feld dann dem Attribut **Geburtsdatum** zu. Um dies zu erreichen, passen Sie das Formular an. Ausführliche Anweisungen über das Hinzufügen eines Felds zu einem Formular finden Sie im *ActiveRoles Server Web-Interface Administratorhandbuch*.

Das Attribut **Geburtstag** kann dann verwaltet werden, indem Personen auf einer Seite des Web-Interface auf Benutzereigenschaften zugreifen. Benutzer können dieses Attribut zum Beispiel über die Site für die Selbstverwaltung anzeigen und ändern, vorausgesetzt, dass die Selbstverwaltung implementiert ist (siehe „Szenario 2: Implementieren der Selbstverwaltung" im Kapitel „Rollenbasierte Administration" weiter oben in diesem Dokument).

Untersuchen von Client-Sitzungen

Auf der ActiveRoles Server-Konsole werden umfassende Informationen zu Client-Sitzungen angezeigt. Wenn die Konsole eine Verbindung mit einem bestimmten Verwaltungsdienst aufweist, können Sie untersuchen, welche Clients diesen Dienst verwenden. Folgende Sitzungsinformationen werden auf der Konsole bereitgestellt:

- **Benutzer** Anmeldename des Kontos, mit dem die Sitzung eine Verbindung mit dem Verwaltungsdienst herstellt.
- **AR Server Admin** Gibt an, ob der Client als Mitglied des Kontos „AR Server Admin" angemeldet ist und somit über Administratorrechte für den Verwaltungsdienst verfügt.
- **Clientversion** Clientanwendung, z.B. MMC-Benutzeroberfläche oder Web-Interface, und ihre Version.
- **Letzter Zugriff** Datum und Uhrzeit des letzten Zugriffs auf den Verwaltungsdienst in dieser Sitzung.
- **Anmeldezeit** Datum und Uhrzeit, zu denen die Sitzung geöffnet wurde.
- **Client Host** DNS-Name (Domain Name System) des Computers, auf dem die Clientanwendung ausgeführt wird.
- **Client Site** Netzwerk-Site des Computers, auf dem die Clientanwendung ausgeführt wird.

Gehen Sie folgendermaßen vor, um eine Liste von Client-Sitzungen für den Verwaltungsdienst anzuzeigen:

1. Stellen Sie eine Verbindung zu dem Verwaltungsdienst her, dessen Client-Sitzungen Sie untersuchen möchten.
2. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration | Server Configuration** und wählen Sie dann **Client Sessions**.

   Daraufhin werden im Bereich „Details" die Client-Sitzungen für den Verwaltungsdienst aufgeführt, mit dem die Konsole verbunden ist.

Mit dem Kontextmenü für eine Clientsitzung können Sie auch folgende Aufgaben ausführen:

- Senden von E-Mail an den Sitzungsbenutzer.
- Trennen der Sitzung vom Verwaltungsdienst.
- Anzeigen zusätzlicher Informationen zur Sitzung.

Um beispielsweise zusätzliche Informationen zu einer Sitzung anzuzeigen, klicken Sie im Bereich „Details" mit der rechten Maustaste auf die Sitzung, und klicken Sie dann auf **Eigenschaften**.

Das Dialogfeld **Eigenschaften** für eine Client-Sitzung umfasst die folgenden Registerkarten:

- **Allgemein** Informationen zum Sitzungsbenutzer, zur Clientversion, zum Clienthost und zur Clientsite.
- **Clientaktivität** Informationen zum Zeitpunkt der Anmeldung, zum Zeitpunkt des letzten Zugriffs sowie zur Anzahl der in der Sitzung ausgeführten Vorgänge, gruppiert nach Vorgangstyp.
- **Mitglied von** Liste aller Sicherheitsgruppen, die aufgrund eines transitiven Erweiterungsvorgangs für die Gruppenmitgliedschaft für den Sitzungsbenutzer zum Zeitpunkt des Sitzungsbeginns berechnet wurden.
- **Domänencontroller** Informationen zu den Domänencontrollern, mit denen Verzeichnisdaten innerhalb der Sitzung abgerufen und aktualisiert werden.

Überwachen der Leistung

ActiveRoles Server enthält eine Reihe von Leistungsindikatoren, mit denen unterschiedliche Leistungsaspekte des Verwaltungsdienstes überwacht werden können. Die Leistungsindikatoren sind in folgenden Leistungsobjekten gruppiert:

- **Anforderungen** Zählt Datenverwaltungsanforderungen, die an den Verwaltungsdienst übermittelt werden.
- **LDAP-Vorgänge** Zählt LDAP-Anforderungen, die vom Verwaltungsdienst ausgegeben werden.
- **Berechtigungsweitergabe** Zählt Änderungen an der Active Directory-Sicherheit, die vom Verwaltungsdienst vorgenommen werden.
- **Externe Änderungen** Zählt Datenänderungen, die der Verwaltungsdienst aus Active Directory abruft, sowie Änderungen, die an der Verwaltungsdatenbank vorgenommen werden.
- **Skriptmodule** Zählt die durchschnittliche Ausführungsdauer von ActiveRoles Server-Skriptmodulen, die Anzahl der Ausführungen eines bestimmten Skriptmoduls und die Anzahl der aktuell ausgeführten Skriptmodulinstanzen.
- **Verschiedenes** Zählt die Anzahl der mit dem Verwaltungsdienst verbundenen Clients und die Anzahl der in der Warteschlange befindlichen Post-Richtlinienverarbeitungsvorgänge.

Um die Leistungsindikatoren des Verwaltungsdienstes zu untersuchen, können Sie das Tool Leistung auf dem Computer mit dem Verwaltungsdienst verwenden:

1. So öffnen Sie das Tool „Leistung": Klicken Sie auf **Starten** und wählen Sie **Alle Programme | Administrative Tools | Leistung**.
2. Wählen Sie in der Konsolenstruktur **Systemmonitor** aus.
3. Klicken Sie im Bereich „Details", und drücken Sie dann STRG+I, um das Dialogfeld **Zähler hinzufügen** anzuzeigen.
4. Wählen Sie in der Liste im Feld **Leistungsobjekt** einen beliebigen Namen aus, der mit dem Präfix **AR Server** beginnt. Sie können beispielsweise **AR Server:Anforderungen** auswählen.
5. Wählen Sie in der Liste der Leistungsindikatoren einen Eintrag aus. Sie können beispielsweise **Anforderungen/Sek.** auswählen.
6. Klicken Sie auf **Hinzufügen** und dann auf **Schließen**.

Nun zeigt das Tool Leistung die Ausgabe des ausgewählten Leistungsindikators an.

Anpassen der Konsole

Die ActiveRoles Server-Konsole bietet eine bequeme Art, die Objekterstellungsassistenten und die Eigenschaftsseiten in der Konsole zu individualisieren und die Anzeigenamen für Objekttypen und Objekteigenschaften anzupassen. Die Individualisierung erfolgt mittels Active Directory-Objekten, die als *Anzeigebezeichner* bezeichnet werden.

Jedes Anzeigebezeichnerobjekt enthält Informationen, die die verschiedenen Benutzerschnittstellenelemente für einen bestimmten Objekttyp beschreiben. Diese Elemente umfassen (sind jedoch nicht beschränkt darauf) die Seiten des Erstellungsassistenten, die Eigenschaftenseiten und Namen, die für Objekttypen und Eigenschaften in Benutzerschnittstellen verwendet werden.

In den folgenden Abschnitten sind die mit der Individualisierung zusammenhängenden Funktionsmerkmale beschrieben, die auf der Verwendung von Anzeigebezeichner basieren:

- Seite **Andere Eigenschaften** im Objekterstellungsassistenten
- Registerkarte **Andere Eigenschaften** im Dialogfeld **Eigenschaften**
- Anpassen von Anzeigenamen

Seite „Andere Eigenschaften" im Objekterstellungsassistent

In der ActiveRoles Server-Konsole werden Verzeichnisobjekte mit Hilfe von Erstellungsassistenten erstellt. Die Erstellung eines Benutzerkontos startet den Assistenten „Neues Objekt – Benutzer". Die ActiveRoles Server-Konsole ermöglicht nun die Erweiterung der Erstellungsassistenten um eine weitere Seite, die die Angabe weiterer Eigenschaften während des Objekterstellungsprozesses erlaubt.

Die ActiveRoles Server-Konsole erleichtert durch die Verwendung einer separaten Registerkarte im Dialogfeld **Eigenschaften** für Anzeigebezeichnerobjekte die Anzeige oder Änderung der Eigenschaften auf der Assistent-Erweiterungsseite. Die Registerkarte **Andere anzuzeigende Eigenschaften** bietet die Möglichkeit zur Anpassung der auf der Erweiterungsseite der Assistenten zur Objekterstellung enthaltenen Eigenschaften. Wenn keine Eigenschaften für die Aufnahme in die Erweiterungsseite vorhanden sind, wird die Seite nicht angezeigt.

Die Registerkarte **Andere anzuzeigende Eigenschaften** kann verwendet werden, um Eigenschaften zur Erweiterungsseite des Erstellungsassistenten für den Objekttyp, mit dem der Anzeigebezeichner verbunden ist, hinzuzufügen bzw. von ihr zu entfernen. Auf der Registerkarte sind die Objekteigenschaften aufgeführt, die auf der Erweiterungsseite enthalten sind. Sie ermöglicht Ihnen, Änderungen an dieser Liste vorzunehmen.

Gehen Sie wie nachfolgend beschrieben vor, um die Seite **Andere Eigenschaften** zum Assistenten „Neues Objekt – Benutzer" hinzuzufügen. Ebenso können Sie den Erstellungsassistent für einen anderen Objekttyp erweitern, indem Sie einen benutzerdefinierten Anzeigebezeichner für diesen Objekttyp erstellen und konfigurieren. Um zum Beispiel den Assistenten für Gruppen, Computer oder Organisationseinheiten zu erweitern, erstellen und konfigurieren Sie einen benutzerdefinierten Anzeigebezeichner mit dem Namen **Gruppe-Anzeige**, **Computeranzeige** bzw. **Organisationseinheit-Anzeige**.

Beachten Sie, dass bei den Namen der Anzeigebezeichner zwischen Groß- und Kleinschreibung unterschieden wird. Sie müssen den Namen daher genau so eingeben, wie er im Active Directory Schema angegeben ist. Um die Namen der Anzeigebezeichner anzuzeigen, können Sie die Konsole verwenden, um den Container „Active Directory | Configuration Container | Display Specifiers | 409" im Rohansichtsmodus zu untersuchen.

Gehen Sie folgendermaßen vor, um den Assistenten „Neues Objekt – Benutzer" zu erweitern:

1. Öffnen Sie die ActiveRoles Server-Konsole und schalten Sie in den Rohansichtsmodus um (wählen Sie **Ansicht | Modus** und klicken Sie dann auf **Rohmodus** und anschließend auf **OK**).
2. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration | Application Configuration** und wählen Sie den Container **Display Specifiers by ActiveRoles Server (Custom)** aus.
3. Verwenden Sie den Befehl **Alle Aufgaben | Erweiterte Erstellung**, um den entsprechenden lokalen Container im Container **Display Specifiers by ActiveRoles Server (Custom)** zu erstellen.

   *Der benutzerdefinierte Anzeigebezeichner muss in dem lokalen Container erstellt werden, der mit dem lokalen Container Ihrer Umgebung übereinstimmt. Diese lokalen Container werden mit Hilfe der hexadezimalen Darstellung der LCID dieser lokalen Container benannt. Folglich heißt der US-amerikanische/englische lokale Container **409**, der deutsche lokale Container **407**, der japanische lokale Container **411** usw.*

   *Möglicherweise müssen Sie zunächst den entsprechenden lokalen Container unter **Display Specifiers by ActiveRoles Server (Custom)** erstellen. Verwenden Sie hierzu den Befehl **Alle Aufgaben | Erweiterte Erstellung**, um ein Objekt der Klasse **EDS-Anzeigebezeichner-Container** zu erstellen*.

4. Erstellen Sie im lokalen Container den benutzerdefinierten Anzeigebezeichner mit dem Namen **Benutzer-Anzeige**.

   *Verwenden Sie hierzu den Befehl **Alle Aufgaben | Erweiterte Erstellung** für den lokalen Container, um ein Objekt der Klasse **Anzeigebezeichner** zu erstellen. Beachten Sie, dass beim Namen des Anzeigebezeichners zwischen Groß- und Kleinschreibung unterschieden wird. Daher sollten Sie den Namen für den neuen Anzeigebezeichner genau als **Benutzer-Anzeige** und nicht als Benutzeranzeige oder BenutzerAnzeige eingeben.*

5. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf **Benutzer-Anzeige** und klicken Sie dann auf **Eigenschaften**.
6. Rufen Sie die Registerkarte **Andere anzuzeigende Eigenschaften** auf.
7. Fügen Sie eine oder mehrere Eigenschaften zur Liste **Andere Eigenschaften bei der Objekterstellung** hinzu. Klicken Sie dann auf **OK**.
8. Starten Sie den Verwaltungsdienst neu und stellen Sie dann erneut die Verbindung zwischen der Konsole und dem Dienst her, damit die Änderungen wirksam werden.

Als Folge dieser Vorgehensweise umfasst der Assistent „Neues Objekt – Benutzer" eine Extraseite, auf der Sie Werte für die von Ihnen in Schritt 7 ausgewählten Eigenschaften angeben können. Sie können den Assistenten in der ActiveRoles Server-Konsole starten, indem Sie mit der rechten Maustaste auf eine Organisationseinheit in der Konsolenstruktur klicken und dann **Neu | Benutzer** wählen. Folgen Sie den Anweisungen des Assistenten, um die Seite aufzurufen, die die Liste der „Sonstigen" Eigenschaften enthält.

Registerkarte „Andere Eigenschaften" im Dialogfeld „Eigenschaften"

Die ActiveRoles Server-Konsole ermöglicht außerdem, das Dialogfeld **Eigenschaften** für Verzeichnisobjekte um eine Extra-Registerkarte mit der Bezeichnung **Andere Eigenschaften** zu erweitern, was bei Verwendung des Befehls **Eigenschaften** die Verwaltung einer benutzerdefinierten Reihe von Objekteigenschaften ermöglicht.

Die ActiveRoles Server-Konsole erleichtert durch die Verwendung einer separaten Registerkarte im Dialogfeld **Eigenschaften** für Anzeigebezeichnerobjekte die Anzeige oder Änderung der Eigenschaften auf der Registerkarte **Andere Eigenschaften**. Auf diese Weise können Sie die Reihe der auf der Registerkarte **Andere Eigenschaften** enthaltenen Eigenschaften anpassen. Beachten Sie, dass das Dialogfeld **Eigenschaften** die Registerkarte **Andere Eigenschaften** nur dann enthält, wenn anzuzeigende Eigenschaften auf dieser Registerkarte vorhanden sind.

Die Registerkarte **Andere anzuzeigende Eigenschaften** kann verwendet werden, um Eigenschaften zur Registerkarte **Andere Eigenschaften** hinzuzufügen bzw. von ihr zu entfernen, die nur den Objekttyp betreffen, mit dem der Anzeigebezeichner verbunden ist. Auf der Registerkarte **Andere anzuzeigende Eigenschaften** sind die Objekteigenschaften aufgeführt, die auf der Registerkarte **Andere Eigenschaften** für den Objekttyp enthalten sind. Sie ermöglicht Ihnen, Änderungen an dieser Liste vorzunehmen.

Gehen Sie wie nachfolgend beschrieben vor, um die Registerkarte **Andere Eigenschaften** zum Dialogfeld **Eigenschaften** für Benutzerobjekte hinzuzufügen. Ebenso können Sie die Eigenschaftenseiten für einen anderen Objekttyp erweitern, indem Sie einen benutzerdefinierten Anzeigebezeichner für diesen Objekttyp erstellen und konfigurieren. Um zum Beispiel das Dialogfeld **Eigenschaften** für Gruppen, Computer oder Organisationseinheiten zu erweitern, erstellen und konfigurieren Sie einen benutzerdefinierten Anzeigebezeichner mit dem Namen **Gruppe-Anzeige**, **Computeranzeige** bzw. **Organisationseinheit-Anzeige**.

Beachten Sie, dass bei den Namen der Anzeigebezeichner zwischen Groß- und Kleinschreibung unterschieden wird. Sie müssen den Namen daher genau so eingeben, wie er im Active Directory Schema angegeben ist. Um die Namen der Anzeigebezeichner anzuzeigen, können Sie die Konsole verwenden, um den Container „Active Directory | Configuration Container | Display Specifiers | 409" im Rohansichtsmodus zu untersuchen.

Gehen Sie folgendermaßen vor, um das Dialogfeld „Eigenschaften" für Benutzerobjekte zu erweitern:

1. Öffnen Sie die ActiveRoles Server-Konsole und schalten Sie in den Rohansichtsmodus um (wählen Sie **Ansicht | Modus** und klicken Sie dann auf **Rohmodus** und anschließend auf **OK**).
2. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration | Application Configuration** und wählen Sie den Container **Display Specifiers by ActiveRoles Server (Custom)** aus.

3. Verwenden Sie den Befehl **Alle Aufgaben | Erweiterte Erstellung**, um den entsprechenden lokalen Container im Container **Display Specifiers by ActiveRoles Server (Custom)** zu erstellen.

   *Der benutzerdefinierte Anzeigebezeichner muss in dem lokalen Container erstellt werden, der mit dem lokalen Container Ihrer Umgebung übereinstimmt. Diese lokalen Container werden mit Hilfe der hexadezimalen Darstellung der LCID dieser lokalen Container benannt. Folglich heißt der US-amerikanische/englische lokale Container **409**, der deutsche lokale Container **407**, der japanische lokale Container **411** usw.*

   *Möglicherweise müssen Sie zunächst den entsprechenden lokalen Container unter **Display Specifiers by ActiveRoles Server (Custom)** erstellen. Verwenden Sie hierzu den Befehl **Alle Aufgaben | Erweiterte Erstellung**, um ein Objekt der Klasse **EDS-Anzeigebezeichner-Container** zu erstellen*.

4. Erstellen Sie im lokalen Container den benutzerdefinierten Anzeigebezeichner mit dem Namen **Benutzer-Anzeige**.

   *Verwenden Sie hierzu den Befehl **Alle Aufgaben | Erweiterte Erstellung** für den lokalen Container, um ein Objekt der Klasse **Anzeigebezeichner** zu erstellen. Beachten Sie, dass beim Namen des Anzeigebezeichners zwischen Groß- und Kleinschreibung unterschieden wird. Daher sollten Sie den Namen für den neuen Anzeigebezeichner genau als **Benutzer-Anzeige** und nicht als Benutzeranzeige oder BenutzerAnzeige eingeben.*

5. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf **Benutzer-Anzeige** und klicken Sie dann auf **Eigenschaften**.
6. Rufen Sie die Registerkarte **Andere anzuzeigende Eigenschaften** auf.
7. Fügen Sie eine oder mehrere Eigenschaften zur Liste **Andere Eigenschaften auf den Objekteigenschaftsseiten** hinzu. Klicken Sie dann auf **OK**.
8. Starten Sie den Verwaltungsdienst neu und stellen Sie dann erneut die Verbindung zwischen der Konsole und dem Dienst her, damit die Änderungen wirksam werden.

Als Folge dieser Vorgehensweise umfasst das Dialogfeld **Eigenschaften** die Registerkarte **Andere Eigenschaften**, auf der Sie Werte für die von Ihnen in Schritt 7 ausgewählten Eigenschaften anzeigen und bearbeiten können. Sie können diese Registerkarte in der ActiveRoles Server-Konsole aufrufen, indem Sie mit der rechten Maustaste auf ein Benutzerkonto klicken und dann auf **Eigenschaften** klicken.

Anpassen von Anzeigenamen

In Active Directory kann jeder Objekttyp über einen Anzeigenamen verfügen, und jede Eigenschaft eines Objekts kann ebenfalls einen Anzeigenamen haben. In Benutzerschnittstellen werden Anzeigenamen als benutzerfreundliche Namen verwendet, um die Identifikation von Objekttypen und -eigenschaften zu erleichtern. Die Anzeigenamen für einen bestimmten Objekttyp werden in den Anzeigebezeichner-objekten für den entsprechenden Objekttyp gespeichert.

Die ActiveRoles Server-Konsole erleichtert durch die Verwendung einer separaten Registerkarte im Dialogfeld **Eigenschaften** für Anzeigebezeichnerobjekte die Anzeige oder Änderung von Anzeigenamen. Die Registerkarte **Anzeigenamen** bietet eine benutzerfreundliche Methode zur Anpassung von Anzeigenamen für Objekttypen und -eigenschaften.

Die Registerkarte **Anzeigenamen** kann verwendet werden, um den Anzeigenamen für den Objekttyp, mit dem der Anzeigebezeichner verbunden ist, anzugeben oder zu ändern und um Anzeigenamen für die Eigenschaften von Objekten dieses Typs hinzuzufügen, zu ändern oder zu entfernen. Die Eigenschafts-Anzeigenamen werden mit Hilfe einer Liste von Namenspaaren verwaltet, wobei der erste Name der LDAP-Anzeigename einer Eigenschaft, gefolgt vom Anzeigenamen dieser Eigenschaft ist.

Gehen Sie folgendermaßen vor, um den englischsprachigen Anzeigenamen für die Klasse „Benutzerobjekt" innerhalb einer Gesamtstruktur zu ändern:

1. Öffnen Sie die ActiveRoles Server-Konsole und schalten Sie in den Rohansichtsmodus um (wählen Sie **Ansicht | Modus** und klicken Sie dann auf **Rohmodus** und anschließend auf **OK**).
2. Erweitern Sie in der Konsolenstruktur den Eintrag **Active Directory | Configuration Container | Display Specifiers** und wählen Sie den Container **409** aus.
3. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf **Benutzer-Anzeige** und klicken Sie dann auf **Eigenschaften**.
4. Ändern Sie auf der Registerkarte **Anzeigenamen** unter **Anzeigename für Objekttyp** den Anzeigenamen und klicken Sie dann auf **OK**.
5. Starten Sie den Verwaltungsdienst neu und stellen Sie dann erneut die Verbindung zwischen der Konsole und dem Dienst her, damit die Änderungen wirksam werden.

Bei Befolgung dieser Schritte nehmen Sie Änderungen an dem Anzeigebezeichner in Active Directory vor. Ihre Änderungen beeinflussen also nicht nur ActiveRoles Server, sondern auch jede Clientanwendung, die Benutzerobjekte in Active Directory verwalten soll (wie etwa Active Directory-Benutzer und Computer). Wenn nur die Anzeigenamen in den ActiveRoles Server-Client-Schnittstellen angepasst werden sollen, nehmen Sie Änderungen an den benutzerdefinierten Anzeigebezeichnern vor, die sich im Container **Display Specifiers by ActiveRoles Server (Custom)** befinden. Das Dialogfeld **Eigenschaften** für benutzerdefinierte Anzeigebezeichner umfasst auch die Registerkarte **Anzeigenamen**, die es Ihnen ermöglicht, die Anzeigenamen so anzupassen, dass Ihre Änderungen nur die ActiveRoles Server-Umgebung betreffen.

16

Anhang

- Anhang A: Verwenden regulärer Ausdrücke
- Anhang B: Administrative Vorlage für die ActiveRoles Server-Konsole

Anhang A: Verwenden regulärer Ausdrücke

Wen Sie eine Erzeugung und Validierung von Eigenschaften-Richtlinie konfigurieren (siehe „Konfigurieren einer Richtlinie für die Generierung und Validierung von Eigenschaften" weiter oben in diesem Dokument), müssen Sie möglicherweise reguläre Ausdrücke erstellen. In diesem Abschnitt wird die Syntax für reguläre Ausdrücke erläutert.

Ein regulärer Ausdruck ist ein Textmuster, das aus gewöhnlichen Zeichen (z.B. den Buchstaben a bis z) und Sonderzeichen, den so genannten Metazeichen, besteht. Er dient als Vorlage, mit der die Übereinstimmung eines Musters aus Zeichen mit dem zu untersuchenden Zeichenfolgenwert überprüft wird.

Die folgende Tabelle enthält eine Liste von Metazeichen und ihrem Verhalten im Kontext regulärer Ausdrücke, mit denen Eigenschaftsüberprüfungskriterien in ActiveRoles Server erstellt werden können. Um bei einem Metazeichen eine Übereinstimmung mit dem Zeichen selbst zu suchen, stellen Sie ihm einen umgekehrten Schrägstrich (\) voran.

ZEICHEN	DEFINITION
****	Markiert das nächste Zeichen als Sonderzeichen, Literal oder oktales Escapezeichen. So stimmt zum Beispiel „n" mit dem Zeichen „n" überein; \n stimmt mit dem Zeichen für eine neue Zeile überein. Die Abfolge \\ stimmt mit \ überein, und \(stimmt mit (überein.
^	Stimmt mit der Position am Anfang der Eingabezeichenfolge überein.
$	Stimmt mit der Position am Ende der Eingabezeichenfolge überein.
*****	Stimmt mit Null oder mehr Vorkommen des vorstehenden Unterausdrucks überein. Beispielsweise stimmt zo* mit z und zoo überein. * ist äquivalent mit {0,}.
+	Stimmt mit einer oder mehr Vorkommen des vorstehenden Unterausdrucks überein. Beispielsweise stimmt zo+ mit zo und zoo überein, aber nicht mit z. + ist äquivalent mit {1,}.
?	Stimmt mit Null oder einem Vorkommen des vorstehenden Unterausdrucks überein. Beispielsweise stimmt do(es)? stimmt mit der Teilzeichenfolge do in do und in does überein. ? ist äquivalent mit {0,1}.
{n}	n ist eine nicht negative ganze Zahl. Stimmt mit genau n Vorkommen des vorstehenden Unterausdrucks überein. Beispielsweise stimmt o{2} nicht mit dem o in Bob, aber mit den beiden o in food überein.
{n,}	n ist eine nicht negative ganze Zahl. Stimmt mit mindestens n Vorkommen des vorstehenden Unterausdrucks überein. Beispielsweise stimmt o{2,} nicht mit dem o in Bob, aber mit allen o in foooood überein. o{1,} ist äquivalent mit o+. o{0,} ist äquivalent mit o*.
{n,m}	m und n sind nicht negative ganze Zahlen mit n <= m. Stimmt mit mindestens n und höchstens m Vorkommen des vorstehenden Unterausdrucks überein. Beispielsweise stimmt o{1,3} mit den ersten drei o in fooooood überein. o{0,1} ist äquivalent mit o?. Beachten Sie, dass zwischen dem Komma und den Zahlen keine Leerzeichen vorhanden sein dürfen.
?	Wenn dieses Zeichen einem der anderen Quantifizierer (*, +, ?, {n}, {n,}, {n,m}) unmittelbar folgt, wird das Muster genügsam („non-greedy"). Ein genügsames Muster stimmt mit dem kürzesten möglichen Teil der durchsuchten Zeichenfolge überein. Dagegen stimmt ein gieriges („greedy") Muster (der Standard) mit dem längsten möglichen Teil der durchsuchten Zeichenfolge überein. Beispielsweise stimmt in der Zeichenfolge oooo der Ausdruck o+? mit einem einzelnen o überein, o+ dagegen mit allen o.
.	Stimmt mit jedem Einzelzeichen außer \n überein. Für eine Übereinstimmung mit jedem Zeichen einschließlich \n verwenden Sie ein Muster wie [.\n].

ZEICHEN	DEFINITION
( )	Gruppiert einen oder mehrere reguläre Ausdrücke, um einen logischen regulären Ausdruck einzurichten, der aus Unterausdrücken besteht. Wird verwendet, um die Standardrangfolge bestimmter Operatoren außer Kraft zu setzen. Übereinstimmungen mit den Klammerzeichen ( ) erreichen Sie mit \(oder \).
x|y	Stimmt mit x oder y überein. Beispielsweise stimmt z|food mit z oder food überein. (z|f)ood stimmt mit zood oder food überein.
[xyz]	Eine Menge von Zeichen. Stimmt mit einem beliebigen der eingeschlossenen Zeichen überein. Beispielsweise stimmt [abc] mit dem a in plain überein.
[^xyz]	Eine negative Menge von Zeichen. Stimmt mit einem beliebigen nicht eingeschlossenen Zeichen überein. Beispielsweise stimmt [^abc] mit dem p in plain überein.
[a-z]	Ein Bereich von Zeichen. Stimmt mit einem beliebigen Zeichen im angegebenen Bereich überein. Beispielsweise stimmt [a-z] mit jedem Kleinbuchstaben im Bereich von a bis z überein.
[^a-z]	Ein negativer Bereich von Zeichen. Stimmt mit einem beliebigen Zeichen überein, das sich nicht im angegebenen Bereich befindet. Beispielsweise stimmt [^a-z] mit jedem Buchstaben außerhalb des Bereichs von a bis z überein.
\b	Stimmt mit einer Wortgrenze überein, d.h. mit der Position zwischen einem Wort und einem Leerzeichen. Beispielsweise stimmt er\b mit dem er in never, aber nicht mit dem er in verb überein.
\B	Stimmt mit der Abwesenheit einer Wortgrenze überein. Beispielsweise stimmt er\B mit dem er in verb, aber nicht mit dem er in never überein.
\cx	Stimmt mit dem durch x angegebenen Steuerzeichen überein. Beispielsweise stimmt \cM mit dem Steuer-M oder Wagenrücklaufzeichen überein. Der Wert von x muss sich im Bereich A-Z oder a-z befinden. Andernfalls wird angenommen, dass es sich bei c um das Literalzeichen c handelt.
\d	Stimmt mit einem Ziffernzeichen überein. Äquivalent mit [0-9].
\D	Stimmt mit einem Nicht-Ziffernzeichen überein. Äquivalent mit [^0-9].
\s	Stimmt mit einem beliebigen Zeichen für Leerraum überein, einschließlich Leerzeichen, Tabulatorzeichen, Seitenvorschub usw. Äquivalent mit [\f\n\r\t\v].
\S	Stimmt mit einem beliebigen Zeichen überein, das nicht für Leerraum steht. Äquivalent mit [^ \f\n\r\t\v].
\w	Stimmt mit jedem Wortzeichen einschließlich des Unterstrichs überein. Äquivalent mit [A-Za-z0-9_].
\W	Stimmt mit jedem Nicht-Wortzeichen überein. Äquivalent mit [^A-Za-z0-9_].
\xn	Stimmt mit n überein, wobei n ein hexadezimales Escapezeichen ist. Hexadezimale Escapezeichen müssen genau zwei Ziffern umfassen. Beispielsweise stimmt \x41 mit A überein. Ermöglicht die Verwendung von ASCII-Codes in regulären Ausdrücken.

Beispiele für reguläre Ausdrücke

Die folgende Tabelle zeigt einige Beispiele für reguläre Ausdrücke und Übereinstimmungen.

AUSDRUCK	ÜBEREINSTIMMUNGEN	KEINE ÜBEREINSTIMMUNGEN
st.n	Austin und Boston	Webster
st[io]n	Austin und Boston	Stanton
st[^io]n	Stanton	Boston oder Austin
^boston	Boston	South Boston oder North Boston Harbor
ston$	Boston und Galveston	Stonewall
sea|side	Seattle und Seaside und Oceanside	Seoul oder Sidney
dal(l|h)art	Dalhart	Dallas oder Lockhart
il?e$	Etoile und Wylie	Beeville
il*e$	Etoile und Wylie und Beeville	Bellaire
il+e$	Etoile und Beeville	Wylie
ad{2}	Addison und Caddo	Adkins
(la.*){2,}	Highland Village und Lake Dallas	Laredo

Rangfolge

Nachdem Sie einen regulären Ausdruck erstellt haben, wird er ähnlich wie ein arithmetischer Ausdruck ausgewertet. Er wird von links nach rechts sowie anhand einer Rangfolge ausgewertet.

Die folgende Tabelle zeigt die Rangfolge für die unterschiedlichen Operatoren in regulären Ausdrücken, beginnend beim höchsten Rang:

ZEICHEN	BESCHREIBUNG
****	Escapezeichen
(), []	Klammern und eckige Klammern
***, +, ?, {n}, {n,}, {n,m}**	Quantifizierer
^, $, \beliebigesMetazeichen	Anker und Sequenzen
|	Alternative

Anhang B: Administrative Vorlage für die ActiveRoles Server-Konsole

Mit der administrativen Vorlage „ARServer.adm" können Sie Registrierungseinstellungen mit Hilfe von Gruppenrichtlinien steuern. So können Sie das Verhalten und das Aussehen der ActiveRoles Server-Konsole konfigurieren. Mit dieser administrativen Vorlage können Sie:

- Einige Teile der Konsolenbenutzeroberfläche ausblenden.
- Standardeinstellungen für einige Elemente der Benutzeroberfläche festlegen.
- Einstellungen angeben, mit denen Erweiterungs-Snap-Ins bei der ActiveRoles Server-Konsole registriert werden.

Die administrative Vorlage enthält die folgenden Richtlinien:

RICHTLINIE	ERKLÄRUNG
Exchange-Verwaltung ausblenden	Entfernt alle Benutzeroberflächenelemente (Befehle, Assistenten und Dialogfelder), mit denen Eigenschaften und Einstellungen im Zusammenhang mit Exchange verwaltet werden können. Wenn Sie diese Richtlinie aktivieren, können Benutzer mit der ActiveRoles Server-Konsole keine Aufgaben für Exchange ausführen und keine Exchange-Empfängereinstellungen verwalten. Wenn Sie diese Richtlinie deaktivieren oder sie nicht konfigurieren, können Benutzer mit den entsprechenden Berechtigungen mit der ActiveRoles Server-Konsole Aufgaben für Exchange ausführen und Exchange-Empfängereinstellungen verwalten.
Standard-Ansichts-modus festlegen	Gibt den Ansichtsmodus an, in dem die ActiveRoles Server-Konsole gestartet wird. Wenn Sie diese Richtlinie aktivieren, können Sie den Ansichtsmodus in einer Liste auswählen. Wenn die ActiveRoles Server-Konsole gestartet wird, schaltet sie in den ausgewählten Ansichtsmodus um. Benutzer können den Ansichtsmodus mit dem Befehl **Modus** im Menü **Ansicht** ändern.
Konfigurationsknoten ausblenden	Entfernt den Knoten **Configuration** aus der Konsolenstruktur, wenn sich die ActiveRoles Server-Konsole im erweiterten Ansichtsmodus befindet. Wenn Sie diese Richtlinie aktivieren, werden im erweiterten Ansichtsmodus alle Objekte und Container, die im Zusammenhang mit der ActiveRoles Server-Konfiguration stehen, nicht angezeigt. Der Knoten **Managed Units** und sein Inhalt sowie alle erweiterten Objekte und Container von Active Directory werden angezeigt.
Option „Kennwort merken" deaktiveren	Deaktiviert das Kontrollkästchen **Kennwort speichern** im Dialogfeld **Verbindung zum Verwaltungsdienst herstellen**. Wenn Sie diese Richtlinie aktivieren, muss der Benutzer bei jeder Verwendung der Option **Verbinden als: Der folgende Benutzer** auf der ActiveRoles Server-Konsole das Kennwort eingeben. Es kann nicht nach einmaligem Eingeben verschlüsselt und gespeichert werden. Beachten Sie, dass das Speichern von Kennwörtern ein potenzielles Sicherheitsrisiko darstellen kann.
„Verbinden als"-Optionen deaktivieren	Deaktiviert die Optionen **Verbindung als** im Dialogfeld **Verbindung zum Verwaltungsdienst herstellen** einschließlich des Kontrollkästchens **Kennwort speichern**. Wenn Sie diese Richtlinie aktivieren, können die Konsolenbenutzer nur unter ihren Anmeldekonten eine Verbindung zum Verwaltungsdienst herstellen. Bei Anwendung dieser Richtlinie wird die Option **Aktueller Benutzer** unter **Verbindung als** ausgewählt und kann nicht geändert werden.
Standardmäßige Markierung von kontrollierten Objekten aktivieren	Gibt an, ob besondere Symbole als visueller Hinweis auf Objekte verwendet werden sollen, auf die Zugriffsvorlagen, Richtlinienobjekte oder Gruppenrichtlinienobjekte angewendet werden (mit ihnen verknüpft sind). Wenn Sie diese Richtlinie aktivieren, können Sie Kategorien von Objekten auswählen, die standardmäßig mit besonderen Symbolen markiert werden sollen. Benutzer können diese Einstellung mit dem Befehl **Kontrollierte Objekte markieren** im Menü **Ansicht** ändern.

Außerdem stellt die administrative Vorlage Richtlinien bereit, mit denen Sie Erweiterungs-Snap-Ins bei der ActiveRoles Server-Konsole registrieren können. Diese Richtlinien befinde sich im Ordner **Erweiterungs-Snap-ins**. Mit jeder Richtlinie in diesem Ordner wird eines der folgenden Elemente registriert:

RICHTLINIE	ERKLÄRUNG
Namespace-Erweiterungen	Registriert Erweiterungs-Snap-Ins, mit denen der Namespace der ActiveRoles Server-Konsole erweitert wird.
Kontextmenü-erweiterungen	Registriert Erweiterungs-Snap-Ins, mit denen ein Kontextmenü auf der ActiveRoles Server-Konsole erweitert wird.
Symbolleisten-erweiterungen	Registriert Erweiterungs-Snap-Ins, mit denen die Symbolleiste der ActiveRoles Server-Konsole erweitert wird.
Eigenschaftsblatt-erweiterungen	Registriert Erweiterungs-Snap-Ins, mit denen Eigenschaftenblätter auf der ActiveRoles Server-Konsole erweitert werden.
Aufgabenlisten-erweiterungen	Registriert Erweiterungs-Snap-Ins, mit denen eine Aufgabenliste auf der ActiveRoles Server-Konsole erweitert wird.
Erweiterungen anzeigen	Registriert Erweiterungs-Snap-Ins, mit denen einer vorhandenen Ansicht Benutzeroberflächenelemente hinzugefügt werden oder mit denen auf der ActiveRoles Server-Konsole neue Ansichten erstellt werden.

Wenn Sie eine Richtlinie aus dem Ordner **Erweiterungs-Snap-ins** konfigurieren, werden Sie aufgefordert, den Namen und den Wert des hinzuzufügenden Elements anzugeben.

Der Namensparameter bestimmt den Typ des zu erweiternden Knotens. Jeder Typ wird mit Hilfe einer GUID identifiziert. Wenn Sie beispielsweise Benutzerobjekte erweitern möchten, lautet die GUID {D842D417-3A24-48e8-A97B-9A0C7B02FB17}. Informationen zu anderen Knotentypen finden Sie in der ActiveRoles Server SDK and Resource Kit-Dokumentation.

Der Wertparameter bestimmt das hinzuzufügende Erweiterungs-Snap-In. Jedes Snap-In wird mit Hilfe einer GUID identifiziert. Sie können mehrere Snap-Ins hinzufügen, indem Sie ihre GUIDs durch Semikolons getrennt eingeben. Beispielsweise ist folgender Wert möglich:

```
{AD0269D8-27B9-4892-B027-9B01C8A011A1}"Description";{71B71FD3-0C9B-473a-B77B-12FD456FFFCB}"Description"
```

Der Eintrag „Description“ ist optional und kann beliebigen Text enthalten, der das Erweiterungs-Snap-In beschreibt. Er muss in Anführungszeichen eingeschlossen sein.

Installationsanweisungen

Verwenden Sie die folgenden Schritte, um mit dem Gruppenrichtlinien-Editor die administrative Vorlage hinzuzufügen oder zu entfernen:

1. Öffnen Sie das Gruppenrichtlinienobjekt, in dem Sie die administrative Vorlage hinzuzufügen oder entfernen möchten.
2. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste unter **Benutzerkonfiguration** auf **Administrative Vorlagen**.
3. Klicken Sie auf **Hinzufügen/Vorlagen entfernen**.
4. Führen Sie eine der folgenden Aktionen durch:
   - Um die Vorlage hinzuzufügen, klicken Sie auf **Hinzufügen**. Suchen Sie im Dialogfeld **Richtlinienvorlagen** die Vorlagendatei **ARServer.adm**, wählen Sie sie aus und klicken Sie dann auf **Öffnen**.
   - Um die Vorlage zu entfernen, klicken Sie in der Liste **Aktuelle Richtlinienvorlagen** auf die Vorlage **ARServer** und klicken Sie dann auf **Entfernen**.

Nachdem Sie dem Gruppenrichtlinienobjekt die Vorlagendatei hinzugefügt haben, können Sie Richtlinieneinstellungen konfigurieren, indem Sie in der Konsolenstruktur **ActiveRoles Server Snap-in Settings** unter **User Configuration/Administrative Templates** auswählen.

Verknüpfen Sie nach dem Konfigurieren der Richtlinieneinstellungen das Gruppenrichtlinienobjekt mit einer Domäne oder einem Container, die bzw. der die Benutzer der ActiveRoles Server-Konsole enthält. Dies können Sie mit dem Active Directory-Tool „Benutzer und Computer" ausführen. Daraufhin ist die Konsole für die Benutzer gemäß den Richtlinieneinstellungen konfiguriert, die Sie angegeben haben.